

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/001232

International filing date: 28 January 2005 (28.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2004-019461  
Filing date: 28 January 2004 (28.01.2004)

Date of receipt at the International Bureau: 24 March 2005 (24.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/JP 2005/001232

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

01. 2. 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日      2 0 0 4 年   1 月 2 8 日  
Date of Application:

出 願 番 号      特 願 2 0 0 4 - 0 1 9 4 6 1  
Application Number:  
[ST. 10/C]:      [J P 2 0 0 4 - 0 1 9 4 6 1]

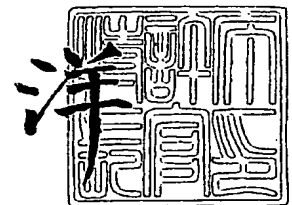
出   願   人      松 下 電 器 産 業 株 式 会 社  
Applicant(s):



特許庁長官  
Commissioner,  
Japan Patent Office

2 0 0 5 年   3 月   9 日

小 川



出証番号   出証特 2 0 0 5 - 3 0 1 9 9 8 6

【書類名】 特許願  
【整理番号】 7048050059  
【提出日】 平成16年 1月28日  
【あて先】 特許庁長官 今井 康夫 殿  
【国際特許分類】 G06F 13/00  
【発明者】  
    【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内  
    【氏名】 大島 京子  
【特許出願人】  
    【識別番号】 000005821  
    【氏名又は名称】 松下電器産業株式会社  
【代理人】  
    【識別番号】 100099254  
    【弁理士】  
    【氏名又は名称】 役 昌明  
【選任した代理人】  
    【識別番号】 100100918  
    【弁理士】  
    【氏名又は名称】 大橋 公治  
【選任した代理人】  
    【識別番号】 100105485  
    【弁理士】  
    【氏名又は名称】 平野 雅典  
【選任した代理人】  
    【識別番号】 100108729  
    【弁理士】  
    【氏名又は名称】 林 紘樹  
【手数料の表示】  
    【予納台帳番号】 037419  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1  
    【包括委任状番号】 9102150  
    【包括委任状番号】 9116348  
    【包括委任状番号】 9600935  
    【包括委任状番号】 9700485

**【書類名】特許請求の範囲****【請求項 1】**

ゲート機器に対して認証処理を行う認証手段と、  
端末にインストールする端末アプリケーションと、  
前記認証手段がゲート機器との認証に成功した場合に、前記ゲート機器から指定された  
端末アプリケーションを端末にインストールする制御手段と  
を備えることを特徴とするセキュアデバイス。

**【請求項 2】**

ゲート機器と端末アプリケーションとの対応関係が規定された対応情報を保持し、前記  
制御手段は、ゲート機器から指定された端末アプリケーションと前記ゲート機器との関係  
が前記対応情報に合致する場合にのみ、前記端末アプリケーションを端末にインストール  
することを特徴とする請求項 1 に記載のセキュアデバイス。

**【請求項 3】**

ゲート機器に対して認証処理を行う認証手段と、  
カードアプリケーションと  
を備え、前記認証手段がゲート機器との認証に成功した場合に、前記ゲート機器から指定  
されたカードアプリケーションが、端末の端末アプリケーションのアクセスを許容すること  
を特徴とするセキュアデバイス。

**【請求項 4】**

前記認証手段が認証に成功したゲート機器と前記ゲート機器から指定されたカードア  
プリケーションとの関係を記録するデータベースを保持し、カードアプリケーションは、端  
末アプリケーションからアクセス要求があったときに、前記データベースの情報に基づい  
て、アクセスの諾否を決定することを特徴とする請求項 3 に記載のセキュアデバイス。

**【請求項 5】**

ゲート機器に対して認証処理を行い、認証に成功したゲート機器の識別情報を登録する  
認証手段と、

前記認証手段がゲート機器との認証に成功したことを条件に所定の動作を行う機器に対  
して、前記機器の検証に供するためにゲート機器の前記識別情報を送信し、または、前記  
機器に代わって前記識別情報を検証するカードアプリケーションと  
を備えることを特徴とするセキュアデバイス。

**【請求項 6】**

前記カードアプリケーションは、前記機器の検証に供するために、入力されたユーザ識  
別情報を前記機器に送信し、または、前記機器に代わって前記ユーザ識別情報を検証す  
ることを特徴とする請求項 5 に記載のセキュアデバイス。

**【請求項 7】**

セキュアデバイスまたは前記セキュアデバイスを保持する端末との通信手段と、  
前記通信手段を通じて前記セキュアデバイスとの認証処理を行い、認証に成功したセキ  
ュアデバイスに対して、端末にインストールする端末アプリケーションを指定するゲート  
アプリケーションと  
を備えることを特徴とするゲート機器。

**【請求項 8】**

セキュアデバイスまたは前記セキュアデバイスを保持する端末との通信手段と、  
前記通信手段を通じて前記セキュアデバイスとの認証処理を行い、認証に成功したセキ  
ュアデバイスに対して、端末の端末アプリケーションがアクセスできるカードアプリケ  
ーションを指定するゲートアプリケーションと  
を備えることを特徴とするゲート機器。

**【請求項 9】**

セキュアデバイスを保持し、ゲート機器との認証に成功した前記セキュアデバイスから  
、前記ゲート機器が指定した端末アプリケーションをインストールすることを特徴とする  
端末装置。

**【請求項 10】**

セキュアデバイスを保持し、ゲート機器との認証に成功した前記セキュアデバイスが保持するカードアプリケーションの中で、前記ゲート機器が指定したカードアプリケーションにアクセスする端末アプリケーションを備えることを特徴とする端末装置。

**【請求項 11】**

前記セキュアデバイスが、着脱可能な状態で装着されていることを特徴とする請求項 9 または請求項 10 に記載の端末装置。

**【請求項 12】**

前記セキュアデバイスが、一体的に埋め込まれていることを特徴とする請求項 9 または請求項 10 に記載の端末装置。

**【請求項 13】**

ゲート機器との認証に成功したセキュアデバイスから前記ゲート機器の識別情報を取得し、前記識別情報の検証に成功した場合に所定の動作を行うことを特徴とする機器。

**【請求項 14】**

ゲート機器との認証に成功したセキュアデバイスから前記ゲート機器の識別情報の検証に成功した旨の情報を取得した場合に所定の動作を行うことを特徴とする機器。

【書類名】明細書

【発明の名称】場所限定サービスを行うセキュアデバイスと装置

【技術分野】

【0001】

本発明は、ＩＣカード等のセキュアデバイスと、このセキュアデバイスとの間で接触通信または非接触通信を行う装置に関し、セキュアデバイスの機能を特定の場所でのみ可能にするものである。

【背景技術】

【0002】

近年、ＩＣカードは、電子決済用カードや定期乗車券、イベント用チケット、クレジットカード等として広く利用されている。最近では、微細化技術の向上とも相俟って、比較的大容量の記憶空間を持つＩＣカードが作られており、このようなＩＣカードは、カードサービスを実行する複数のカードアプリケーション（以下、アプリケーションを「アプリ」と略称する）を格納することにより、一枚で複数の用途に対応するマルチアプリカードとして使用することができる。

【0003】

ＩＣカードの通信方式には、ＩＣカードの電氣的接点にリーダ・ライタを接触して記録情報の読み書きを行う接触通信と、無線通信で情報をやり取りし、リーダ・ライタとの物理的な接触を必要としない非接触通信との二通りがある。最近では、接触通信及び非接触通信の両方が可能なＩＣカード（コンピカード）を携帯端末装置に搭載し、この携帯端末を電子財布や定期券の替わりに使用することも行われている。

【0004】

下記特許文献１には、搭載したマルチアプリカードから、目的のカード機能を迅速かつ簡単に選択することを可能にした携帯端末装置が開示されている。この装置を使用するユーザは、マルチアプリカードのカード機能を携帯端末の表示画面に一覧表示して、その中から親アプリと、親アプリに関連付けたアプリ（優先アプリ）とを登録し、マルチアプリカードに記憶させる。例えば、親アプリとして定期乗車券機能を登録し、その優先アプリとして電子マネー機能を登録すると、携帯端末を自動改札装置に翳し、マルチアプリカードの定期乗車券機能を用いて駅構内に入場した場合に、携帯端末の表示画面には、優先アプリの電子マネー機能の表示順位を最上位に設定したアプリ選択画面が表示される。

【0005】

また、ユーザがマルチアプリカードのアプリ機能を使用すると、その位置が携帯端末のＧＰＳ受信機等の現在位置検出手段で検出されて、使用したアプリ機能と使用位置との関係が携帯端末で記憶される。そして、その位置付近を再び訪れたとき、携帯端末の表示画面には、その位置に対応するアプリ機能の表示順位を最上位に設定したアプリ選択画面が表示される。

【特許文献１】特開 2003-76958 号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

このように、場所と対応付けてアプリ選択画面の表示を変更することは前記特許文献１に記載されているが、ＩＣカードのカード機能を場所によって限定する発想は、この文献には示されていない。ＩＣカードのカード機能を場所で限定することができるならば、例えば、ＩＣカードを搭載した携帯電話を、社内エリアでは内線電話として使用できるようにし、あるいは、ＩＣカードに格納された特定データを社内エリアでのみ利用できるようにする等、新たな応用が可能になる。

【0007】

また、ＩＣカードのカード機能を場所によって限定する場合に、前記特許文献１のように、ユーザの登録操作を必要とするのでは、ユーザの処理負担が大きいし、また、携帯端末が位置情報の取得手段を持つ必要があるのでは、携帯端末のコストが高くなる。

## 【0008】

本発明は、こうした従来の課題を解決するものであり、ユーザの処理負担やコスト負担を招かずに、カードアプリ機能や装置機能等が発現されるエリアを限定することができるＩＣカード等のセキュアデバイスを提供し、また、このセキュアデバイスと連携して処理を行う装置を提供することを目的としている。

## 【課題を解決するための手段】

## 【0009】

本発明では、セキュアデバイスに、ゲート機器に対して認証処理を行う認証手段と、端末にインストールする端末アプリと、認証手段がゲート機器との認証に成功した場合に、ゲート機器から指定された端末アプリを端末にインストールする制御手段とを設けている。

そのため、セキュアデバイスをゲート機器に繋し、正常に通過したエリアでのみ、端末アプリが端末にインストールされる。ゲート機器のゲートアプリが特定の領域で機能するアプリを指定するので、ユーザの登録操作等は不要であり、また、端末へのＧＰＳ受信機等の装備も必要がない。

## 【0010】

また、本発明では、セキュアデバイスに、ゲート機器に対して認証処理を行う認証手段と、カードアプリとを設け、認証手段がゲート機器との認証に成功した場合に、ゲート機器から指定されたカードアプリが、端末の端末アプリのアクセスを許容するようにしている。

そのため、セキュアデバイスをゲート機器に繋し、正常に通過したエリアでのみ、端末アプリは、カードアプリの利用が可能になる。

## 【0011】

また、本発明では、セキュアデバイスに、ゲート機器に対して認証処理を行い、認証に成功したゲート機器の識別情報を登録する認証手段と、認証手段がゲート機器との認証に成功したことを条件に所定の動作を行う機器に対して、この機器の検証に供するためにゲート機器の識別情報を送信し、または、この機器に代わって識別情報を検証するカードアプリとを設けている。

そのため、ゲート機器が設置された正規の入口から入場しないと、機器は動作しない。

## 【0012】

また、本発明では、ゲート機器に、セキュアデバイスまたはセキュアデバイスを保持する端末との通信手段と、通信手段を通じてセキュアデバイスとの認証処理を行い、認証に成功したセキュアデバイスに対して、端末にインストールする端末アプリを指定するゲートアプリとを設けている。

また、ゲート機器に、セキュアデバイスまたはセキュアデバイスを保持する端末との通信手段と、通信手段を通じてセキュアデバイスとの認証処理を行い、認証に成功したセキュアデバイスに対して、端末の端末アプリがアクセスできるカードアプリを指定するゲートアプリとを設けている。

そのため、認証に成功したセキュアデバイスに対して、端末にインストールする端末アプリや、端末アプリがアクセス可能となるカードアプリを指定することができる。

## 【0013】

また、本発明の端末装置は、セキュアデバイスを保持し、ゲート機器との認証に成功したセキュアデバイスから、ゲート機器が指定した端末アプリをインストールするように構成している。

また、端末装置は、セキュアデバイスを保持し、ゲート機器との認証に成功したセキュアデバイスが保持するカードアプリの中で、ゲート機器が指定したカードアプリにアクセスする端末アプリを備えている。

そのため、入口にゲート機器が設置された特定のエリアの中でのみ、端末装置の特殊な機能が発揮できる。

## 【0014】

また、本発明では、機器が、ゲート機器との認証に成功したセキュアデバイスからゲート機器の識別情報を取得し、この識別情報の検証に成功した場合に所定の動作を行うように構成している。

また、機器が、ゲート機器との認証に成功したセキュアデバイスからゲート機器の識別情報の検証に成功した旨の情報を取得した場合に所定の動作を行うように構成している。

そのため、ユーザがセキュアデバイスを所持して正規の入口から入場しないと、機器は動作しない。

#### 【発明の効果】

##### 【0015】

本発明のセキュアデバイス、ゲート機器、端末装置及び機器は、連携して、セキュアデバイスのカード機能や、端末装置あるいは機器の機能を、場所と関連付けて変更することができる。例えば、端末装置の機能をオフィスの中と外とで切替えたり、特定の処理機能を限定したエリアでのみ可能にしたり、特定の入口から入場しなければ、部屋の扉や金庫が開かないようにしたりすることができる。

また、こうした処理を、ユーザの処理負担やコスト負担を招かずに実現することができる。

#### 【発明を実施するための最良の形態】

##### 【0016】

##### (第1の実施形態)

本発明の第1の実施形態では、ICカードが特定エリアに位置するときだけ、ICカードに格納された端末アプリが、端末にインストールされる場合について説明する。

この特定エリアの入口にはゲートが在り、ゲートアプリは、ICカードとの認証処理に成功すると、ICカードに対して、端末に設定すべき端末アプリを指定する。これを受けて、ICカードは、適宜の時期に、保持する端末アプリの中から、指定された端末アプリを端末にインストールする。

##### 【0017】

図1は、端末(機器1)が携帯電話10であり、ICカード(機器2)が、携帯電話10に装着されたチップ状のコンビカード20である場合の、携帯電話10、コンビカード20及びゲート40(機器3)の構成について示している。

ゲート40は、コンビカード20に対して認証処理や端末アプリの指定を行うゲートアプリ43と、コンビカード20への非接触通信を行う非接触通信手段(4)41と、ゲート40の動作を制御するCPU42とを備えている。

コンビカード20は、ゲート40への非接触通信を行う非接触通信手段(3)22と、携帯電話10への接触通信を行う接触通信手段(2)21と、認証情報等が格納された認証情報データベース(DB)25と、他の機器1、3との認証処理を行う認証アプリ24と、携帯電話10にインストールする端末アプリ27や設定命令、あるいはそれらのセット26と、コンビカード20の動作を制御するCPU23とを備えている。

また、携帯電話10は、コンビカード20への接触通信を行う接触通信手段(1)11と、携帯電話10の動作を制御するCPU12とを備えている。

##### 【0018】

このコンビカード20の認証情報DB25には、図2に示すように、ゲートアプリ43のIDと対応付けて、認証処理に使用する共通鍵や秘密鍵等の認証情報と、携帯電話10へのインストールが可能な端末アプリ27のIDや、携帯電話10で設定すべき端末アプリを指定する設定命令のIDが格納されている。

##### 【0019】

設定命令は、例えば、携帯電話10に対する次のような指示である。

- ・表示画面の背景イメージに会社ロゴを設定する。
- ・音(着信時、アプリ実行時)に会社用の音を設定する。
- ・メインメニューに、社内で使用するイントラネットアプリを追加する。
- ・デフォルトを内線電話に変更する(外線への発信を0発信に変更)。



また、携帯電話10へのインストールが可能な端末アプリは、携帯電話10で保持されていない、設定命令の実行に必要なアプリであり、例えば、設定命令に基づく表示を実行するブラウザ等のソフトウェアである。

#### 【0020】

図3は、このゲート40、コンビカード20及び携帯電話10が連携して行う処理のシーケンスを示している。

ユーザは、所定エリアに入場する際に、コンビカード20を装着した携帯電話10をゲート40に翳す。ゲート40のCPU42は、非接触通信手段41の通信圏内にコンビカード20が進入すると、コンビカード20に認証アプリIDとゲートアプリIDとを指定して認証処理を要求する(1-1)。これを受けてコンビカード20のCPU23は認証アプリ24を起動し、認証アプリ24は、認証情報DB25のゲートアプリIDに対応する認証情報を用いて、ゲートアプリ43との間で、一般的なチャレンジレスポンスによる認証処理を実行する(1-2)。認証処理に成功すると、ゲートアプリ43は、端末アプリIDを指定して、その端末アプリの端末へのインストールを要求する(1-3)。指定する端末アプリIDは複数であっても良い。

#### 【0021】

この要求を受けたコンビカード20の認証アプリ24は、認証情報DB25の情報から、その端末アプリがインストール可能であることを確認(検証)し、その旨をCPU23に伝える。CPU23は、携帯電話10に端末アプリIDを示してインストール要求を送り(2-1)、認証アプリ24に携帯電話10との認証処理を行わせる(2-2)。なお、コンビカード20を携帯電話10に装着した時点で両者間の認証処理が既に済んでいれば、この認証処理を省略しても良い。認証処理に成功すると、CPU23は、該当する端末アプリ26、27を携帯電話10に送信し(2-3)、携帯電話10のCPU12は、その端末アプリをインストールする。

#### 【0022】

このように、このゲート40、コンビカード20及び携帯電話10の間では、三者の連携により、コンビカード20とゲート40との認証の成功を条件に、コンビカード20から携帯電話10への端末アプリのインストールが実行される。そのため、このコンビカード20の動作や、携帯電話10の端末アプリを利用する処理は、ゲート40を通過して入場したエリアでのみ可能になる。

#### 【0023】

なお、ICカードの国際標準規格(接触通信に関するISO7816、非接触通信に関するISO14443)では、ICカードのカードアプリとリーダー・ライター側の端末アプリとのデータのやり取りは、端末アプリからカードアプリに送られる「コマンド」と、カードアプリから端末アプリに送られる「レスポンス」とが基本になると規定されている。従って、国際標準規格を満たすICカードは、受動的な動作しかできず、(2-1)のインストール要求を自ら携帯電話10に送信することができない。

そのため、携帯電話10は、国際標準規格を満たすコンビカード20の場合には、ユーザが携帯電話10をゲート40に翳した時点から、非接触通信の状態を監視するためにコンビカード20にポーリング信号を送り続ける。そして、コンビカード20から非接触通信終了の応答を受けると、コンビカード20に対し、要求があれば送信するように指示し、コンビカード20は、これに応じてインストール要求を携帯電話10に送信する(2-1)。

こうした手順を採ることにより、国際標準規格を満たすICカードにも対応することができる。

#### 【0024】

なお、ここでは、ICカードがコンビカードである場合について説明したが、ICカードが接触通信機能のみを有するときは、図4に示すように、携帯電話10の赤外線(またはBluetoothや無線LAN)等のローカル通信手段13を利用して、ICカード20とゲート40との通信を行うことができる。この場合、ゲート40が、通信手段44

と携帯電話 10 のローカル通信手段 13 との通信 (赤外線) 接続を確立して、携帯電話 10 に IC カード 20 へのアクセス命令を送ると、携帯電話 10 は IC カード 20 との接触通信接続を実行し、ゲート 40 と IC カード 20 との通信が可能になる。ゲート 40、IC カード 20 及び携帯電話 10 の三者間におけるデータのシーケンスは、図 3 と同じである。

#### 【0025】

また、IC カードが非接触通信機能のみを有するときには、携帯電話 10 およびゲート 40 と非接触通信を用いて通信を行う。ユーザが携帯電話 10 をゲート 40 に翳した時点から、ゲート 40 との処理状態を監視するために非接触 IC カード 20 に問合せを行う。そして、非接触 IC カード 20 は、ゲート 40 との処理が終了すると、携帯電話 10 に終了通知を返し、この結果携帯電話 10 は非接触 IC カード 20 に対し、要求があれば送信するように指示し、非接触 IC カード 20 は、これに応じてインストール要求を携帯電話 10 に送信する (2-1)。または、非接触 IC カード 20 は、ゲート 40 との処理が終了すると、携帯電話 10 に終了通知とともにインストール要求を携帯電話 10 に送信する (2-1)。

#### 【0026】

##### (第 2 の実施形態)

本発明の第 2 の実施形態では、IC カードとゲートとの認証成功を条件に、IC カードに格納されたカードアプリの利用が、端末に対して許可される場合について説明する。

ゲートは、IC カードとの認証に成功すると、IC カードに、端末での利用を許容するカードアプリの ID と、ゲートを特定するゲート PIN 情報とを伝え、このカードアプリ ID とゲート PIN との対情報が IC カードに格納される。IC カードは、端末からカードアプリを指定して、その利用が要求されたとき、この対情報を参照して、カードアプリの利用を許可するか否かを決定する。

#### 【0027】

図 5 は、この処理を連携して行う携帯電話 10、コンビカード 20 及びゲート 40 の構成について示している。コンビカード 20 は、第 1 の実施形態 (図 1) と同様に、非接触通信手段 (3) 22、接触通信手段 (2) 21、認証情報 DB 25、認証アプリ 24 及び CPU 23 を備え、さらに、ゲート 40 との認証に成功した場合に有効になるカードアプリ 28 と、カードアプリ ID とゲート PIN との対情報を格納する PIN DB 29 とを備えている。また、携帯電話 10 は、接触通信手段 (1) 11、CPU 12 の他に、カードアプリ 28 を利用する端末アプリ 14 を備えている。ゲート 40 の構成は第 1 の実施形態 (図 1) と変わりが無い。

#### 【0028】

このコンビカード 20 の認証情報 DB 25 には、図 6 に示すように、ゲートアプリ 43 の ID と対応付けて、認証処理に使用する認証情報と、ゲート PIN の設定が可能な (即ち、ゲート 40 から入場したエリアで利用可能な) カードアプリの ID と、PIN 設定を解除する (即ち、そのエリアで利用できなくなる) カードアプリの ID とが格納されている。

ゲート 40 から入場したエリアで利用可能になるカードアプリ 28 は、例えば、所内の内線番号電話帳アプリであり、コンビカード 20 とゲート 40 との認証が成功すると、携帯電話 10 の電話帳機能を実行する端末アプリ 14 からコンビカード 20 に格納された内線簿にアクセスできるようになる。

#### 【0029】

図 7 は、このゲート 40、コンビカード 20 及び携帯電話 10 が連携して行う処理のシーケンスを示している。

ユーザがコンビカード 20 を装着した携帯電話 10 をゲート 40 に翳すと、ゲート 40 は、コンビカード 20 に認証アプリ ID とゲートアプリ ID とを示して相互間の認証処理を要求する (1-1)。これを受けてコンビカード 20 の認証アプリ 24 は、認証情報 DB 25 のゲートアプリ ID に対応する認証情報を用いて、ゲートアプリ 43 との認証処理

を実行する(1-2)。認証処理に成功したゲートアプリ43は、ゲートPINを設定したい(または削除したい)カードアプリのIDとゲートPINとを提示して、カードアプリIDとゲートPINとの対情報の登録(または削除)を認証アプリ24に要求する(1-3)。このときゲートアプリ43が提示するカードアプリIDの数は、複数であっても良い。

#### 【0030】

コンビカード20の認証アプリ24は、そのカードアプリIDに該当するカードアプリ28にゲートアプリIDとゲートPINとの情報を送り、確認(検証)を要求する(2-1)。カードアプリ28は、認証情報DB25を参照して、ゲートアプリとの対応関係を有しているか否か(ゲートPINの設定が可能であるか否か)を検証し、検証結果を認証アプリ24に返す(2-2)。認証アプリ24は、検証結果がOKである場合に、検証されたカードアプリIDとゲートPINとの対情報をPINDB29に格納し(2-3)、検証結果をゲートアプリ43に通知する(2-4)。

以上がゲート通過時に行われる処理である。

#### 【0031】

一方、携帯電話10の端末アプリ14がカードアプリ24を利用する場合には、次の処理が行われる。

携帯電話10の端末アプリ14は、カードアプリIDを提示して、コンビカード20のカードアプリ28にアクセスを要求する(3-1)。カードアプリ28は、認証アプリ24に、カードアプリIDを示して検証結果を要求する(3-2)。認証アプリ24は、PINDB29を参照し、そのカードアプリIDとゲートPINとの対情報が記録されているときはOKを応答し、記録されていないときはNGを応答する(3-3)。カードアプリ28は、認証アプリ24からの応答がOKである場合に、端末アプリ14に対してアクセスを許可する(3-5)。

#### 【0032】

こうした処理により、ユーザが正しいゲート40から入場した場合にのみ、カードアプリ28の利用を可能にすることができ、例えば、ユーザがICカードを装着した携帯電話を正規のゲートに翳してオフィスに入場すると、ICカードに格納されたオフィス用の内線番号電話帳アプリが自動的に有効になる。

#### 【0033】

なお、ゲートアプリ43から提示されたカードアプリIDがPIN設定を解除するカードアプリIDとして認証情報DB25に記録されている場合には、認証アプリ24は、PINDB29を参照し、そこに記録されているカードアプリIDとゲートPINとの対情報を削除する。

このようにPINDB29の削除処理を併せて行うことにより、例えば、ユーザが、入門処理をして、あるオフィスに入場した後、別のオフィスに入門処理をして入場した場合に、先のオフィス用の内線番号電話帳アプリが無効になり、後から入場したオフィス用の内線番号電話帳アプリだけが有効になる。

#### 【0034】

なお、各処理のメッセージ及びデータは、第三者の盗聴を防ぐために暗号化して送信するようにしても良い。

また、図7において、(2-3)の検証結果の格納は、カードアプリIDの検証結果がOKであることを示す情報だけをPINDB29に格納するようにしても良い。

また、ICカードは、接触通信機能のみを有するものであっても良い。この場合には、第1の実施形態(図4)で説明したように、携帯電話10のローカル通信手段を利用してICカードとゲートとの通信を行う。

また、ICカードは、非接触通信機能のみを有するものであっても良い。

#### 【0035】

なお、図6に示す認証情報DBにおいて、一つのゲートアプリIDに対し、複数のカードアプリIDが設定されている場合には、端末アプリのアクセスを許容するカードアプリ

に優先度を設定することも可能である。この場合、図8に示すように、ゲートアプリIDに対応して、優先度設定可能なカードアプリID及び優先度設定を解除できるカードアプリIDの優先度を設定した優先設定DBを保持する。あるいは、図9に示すように、各カードアプリIDの優先度を優先度テンプレート(b)で規定し、ゲートアプリIDに対応して優先度テンプレートを設定した優先設定DB(a)を保持する。

そして、認証情報DBから、ゲートアプリIDに対応するカードアプリを選択する場合に、優先設定DBを参照し、優先度に基づいて選択するカードアプリを決定する。

#### 【0036】

(第3の実施形態)

本発明の第3の実施形態では、ICカードとゲートとの認証成功を条件に、ICカードに格納されたカードアプリの利用が、端末に対して許可される第2の実施形態の構成において、ICカード、ゲート及び端末の三者間での処理が、第2の実施形態と異なる手順で行われる場合について説明する。

#### 【0037】

ここでは、図10に示すように、機器1が、非接触通信手段(1)110を有するドア100であり、機器2が、非接触通信手段22のみを有するICカード200であるものとして説明する。機器1、機器2及び機器3のその他の構成は、第2の実施形態(図5)と変わりがない。

ここでは、非接触通信手段22のみを有するが、接触通信手段のみを有しても良い。

#### 【0038】

図11は、ゲート40、ICカード200及びドア100が連携して行う処理のシーケンスを示している。

ユーザがICカード200をゲート40に翳すと、ゲート40は、ICカード200に認証アプリIDとゲートアプリIDとを示して相互間の認証処理を要求する(1-1)。これを受けてICカード200の認証アプリ24は、認証情報DB25のゲートアプリIDに対応する認証情報を用いて、ゲートアプリ43との認証処理を実行する(1-2)。認証処理に成功したゲートアプリ43は、ゲートPINを設定するカードアプリのIDとゲートPINとを提示して、カードアプリIDとゲートPINとの対情報の登録を認証アプリ24に要求し(1-3)、ICカード200の認証アプリ24は、要求に従ってカードアプリIDとゲートPINとの対情報をPINDB29に登録する(1-4)。この登録の段階では、認証情報DB25との検証は済んでいない。

以上がゲート通過時に行われる処理である。

#### 【0039】

一方、ユーザがICカード200をドア100に翳すと、次の処理が行われる。

ドア100の端末アプリ14は、端末アプリIDとカードアプリIDとを提示して、ICカード200のカードアプリ28へのアクセスを要求する(2-1)。カードアプリ28は、認証アプリ24に、カードアプリIDとゲートアプリIDとを示してPINDB29の登録情報を要求し(2-2)、認証アプリ24は、PINDB29から、該当するカードアプリID及びゲートPINの対情報を取得してカードアプリ28に提示する(2-3)。カードアプリ28は、認証情報DB25を参照して、ゲートアプリとの対応関係を有しているか(ゲートPINの設定が可能であるか)を検証し(2-4)、検証結果がOKである場合に、端末アプリ14にアクセスを許可する(2-5)。

カードアプリ28にアクセスしたドア100の端末アプリ14は、例えば、カードアプリ28から鍵情報を取得してドア100を開錠し、ユーザは、ドア100の通過が可能になる。

#### 【0040】

このように、ゲート40、ICカード200及びドア100が連携することにより、正しい玄関(ゲート)から入らないと、ドアが開かないようにすることができる。

また、このPIN検証(2-4)では、カードアプリ28が、端末アプリ14とゲートPINとのペアを検証することも可能であり、この場合には、ある端末アプリ14につい

て、特定のゲートPINと対応していなければアクセスを許可しない（即ち、あるドアは特定の入口から入らないと開かない）と言う制御を行うこともできる。

#### 【0041】

また、図12に示すように、ドア100にPIN入力部15を設け、ユーザがPIN入力部15から入力したユーザPINをさらに検証して、ドア100を開けるように制御することもできる。

図13は、この場合のシーケンスを示している。ゲートPINを検証する（2-4）までの処理は、図11の場合と同じである。ゲートPINの検証結果がOKである場合に、カードアプリ28は、ドア100にユーザPINを要求し（2-5）、ユーザがPIN入力部15からユーザPINを入力すると（2-6）、カードアプリ28は、ICカード200のPINDB29で保持されたユーザPINと照合して、それを検証する（2-7）。そして、検証結果が一致する場合に、端末アプリ14に対してアクセスを許可する（2-8）。

#### 【0042】

##### （第4の実施形態）

本発明の第4の実施形態では、ICカードとゲートとの認証処理が成功したことを条件に、機器の処理が可能になる場合について説明する。

ICカードは、ゲートとの認証処理が成功すると、ゲートからゲートPINを取得し、このゲートPINを機器に送信する。機器は、ゲートPINの検証が終了した後、処理を開始する。

#### 【0043】

図14は、ゲート40、コンビカード20及び携帯電話10の構成と、機器（機器4）が金庫50である場合の構成とを示している。このコンビカード20を装着した携帯電話10をゲート40に翳し、コンビカード20とゲート40との認証処理を行う。認証が成功した場合に、この携帯電話10を金庫50に翳し、また、携帯電話10からユーザPINを入力することにより、金庫50の開錠が可能になる。

金庫50は、コンビカード20への非接触通信を行う非接触通信手段（5）51と、金庫50の鍵の開閉を制御する鍵アプリ53と、金庫50の動作を制御するCPU52とを備えている。ゲート40、コンビカード20及び携帯電話10の構成は、第2の実施形態（図10）と変わりが無い。

#### 【0044】

コンビカード20を装着した携帯電話10をゲート40に翳すと、ゲート40とコンビカード20との間で、図13の（1-1）から（1-4）までの処理が行われる。

図15は、その後、ユーザが、コンビカード20を装着した携帯電話10を金庫50に翳したときの処理シーケンスを示している。

金庫50の鍵アプリ53は、カードアプリIDを示して、コンビカード20にカードアプリ29へのアクセスを要求する（3-1）。カードアプリ29は、カードアプリID及び鍵アプリIDを提示して、認証アプリ24にゲートPINを要求する（3-2）。認証アプリ24は、PINDB29を参照し、カードアプリIDに対応するゲートPIN情報を取得してカードアプリ29に返す（3-3）。

#### 【0045】

次に、カードアプリ29は、携帯電話10の端末アプリ14にユーザPINを要求する（3-4）。端末アプリ14は、PIN入力画面を表示し、ユーザがPINを入力すると（3-5）、そのユーザPINをカードアプリ29に送信する（3-6）。カードアプリ29は、コンビカード20のPINDB29で保持されているユーザPIN情報と照合して、それを検証する（3-7）。ユーザPINの検証結果が一致した場合は、ゲートPINを金庫の鍵アプリ53に送信する（3-8）。鍵アプリ53は、予め保持するゲートPIN情報と、カードアプリ29から送られたゲートPINとを照合して検証し（3-9）、検証結果が一致する場合に、開錠処理を実行する（3-10）。

このように、例えば、ゲート40が玄関に設置されている場合では、玄関での入門処理

が正しく行われたときにのみ、金庫50の鍵が使えることになる。

【0046】

なお、ユーザPINやゲートPINの検証を行う時期、あるいは、検証を行う主体等については、種々の変更が可能である。例えば、鍵アプリ53がゲートPINの検証(3-9)を行う代わりに、カードアプリ29が、ユーザPIN検証(3-8)とともに、ゲートPINの検証を行い、検証結果を鍵アプリ53に伝えるようにしても良い。

また、カードアプリ29がユーザPIN検証(3-8)を行う代わりに、入力されたユーザPINを鍵アプリ53に送り、鍵アプリ53が、金庫50に登録されたユーザPINと照合してユーザPIN検証を行うようにしても良い。

【0047】

また、図16に示すように、PIN登録(4-4)を終了した認証アプリ24が、端末アプリ14にユーザPINを要求し(4-5)、入力されたユーザPINをそのままPINDB29に登録(4-8)するようにしても良い。この場合は、図17に示すように、携帯電話10を金庫50に繋いだ段階で、カードアプリ29が、PINDB29からゲートPIN及びユーザPINを取得し(5-3)、ユーザPINを検証し(5-4)、ゲートPINを金庫50の鍵アプリ53に送る(5-5)。この方式では、ユーザのPIN入力が事前に済んでいるため、金庫50の前でのユーザの入力操作が不要になる。

【0048】

また、図18に示すように、PIN登録(4-4)が終了した時点で、その通知を受けたカードアプリ28が、ユーザPINを要求し(4-6)、入力されたユーザPINを検証して(4-8)、検証結果を登録する(4-10)ようにしてもよい。この場合は、図19に示すように、携帯電話10を金庫50に繋いだ段階で、ユーザの検証結果をチェックする(5-4)だけで足りる。この方式では、ユーザPIN検証が早い段階で行われるため、ユーザがPIN入力を間違えていた場合に、早い段階で修正できる。

【0049】

また、図20は、コンビカード(機器2)のカードアプリ(アプリ2)が、ユーザPIN要求と、ゲートPIN検証と、ユーザPIN検証とを行う場合のシーケンスを示している。

また、図21は、コンビカード(機器2)のカードアプリ(アプリ2)が、ユーザPIN要求と、ユーザPIN検証とを行い、金庫(機器4)の鍵アプリ(アプリ5)がゲートPIN検証を行う場合のシーケンスを示している。

また、図22は、コンビカード(機器2)のカードアプリ(アプリ2)が、ユーザPIN要求と、ゲートPIN検証とを行い、金庫(機器4)の鍵アプリ(アプリ5)がユーザPIN検証を行う場合のシーケンスを示している。

【0050】

また、図23は、コンビカード(機器2)の認証アプリ(アプリ3)が、ユーザPIN要求を行い、金庫(機器4)の鍵アプリ(アプリ5)がゲートPIN検証と、ユーザPIN検証とを行う場合のシーケンスを示している。

また、図24は、ユーザPIN入力を金庫(機器4)から行い、金庫(機器4)の鍵アプリ(アプリ5)がゲートPIN検証と、ユーザPIN検証とを行う場合のシーケンスを示している。

また、図25は、ユーザPIN入力を金庫(機器4)から行い、コンビカード(機器2)のカードアプリ(アプリ2)が、ユーザPIN検証を行い、金庫(機器4)の鍵アプリ(アプリ5)がゲートPIN検証を行う場合のシーケンスを示している。

また、図26は、ユーザPIN入力を金庫(機器4)から行い、コンビカード(機器2)のカードアプリ(アプリ2)が、ゲートPIN検証を行い、金庫(機器4)の鍵アプリ(アプリ5)がユーザPIN検証とを行う場合のシーケンスを示している。

【0051】

コンビカード(機器2)のカードアプリ(アプリ2)でゲートPINを検証する場合は、ゲートPINが変わった場合に、カード内に格納されたゲートPINを変更すれば足り

る。また、ゲートアプリ（アプリ 4）と鍵アプリ（アプリ 5）の組み合わせでアクセス制御を行うことができる。

また、金庫（機器 4）の鍵アプリ（アプリ 5）でゲート PIN を検証する場合は、新しい金庫（機器 4）が追加された時に、その金庫にゲート PIN 情報を登録するだけで足りる。また、金庫を削除するときに、カードの設定を変える必要がない。

#### 【0052】

また、コンビカード（機器 2）のカードアプリ（アプリ 2）でユーザ PIN を検証する場合は、ユーザがユーザ PIN を変えたい場合に、コンビカード（機器 2）に格納されているユーザ PIN を変更するだけで足り、わざわざユーザ PIN を換えたい機器（例えば金庫）のところに赴いて変えなくても済む。また、一つのユーザ PIN が複数の機器（ドアなど）に対応している場合でも、ドアごとにユーザ PIN を設定して回らなくて済む。また、図 18 に示すように、ユーザ PIN を事前入力する場合に、ユーザ PIN の入力時に金庫（機器 4）無しで検証が行えるので、金庫に繋してからユーザ PIN の再入力が必要になるような事態は発生しない。

また、金庫（機器 4）の鍵アプリ（アプリ 5）でユーザ PIN を検証する場合は、金庫でユーザ PIN を管理しているので、何人のユーザが登録されているのかが容易に把握できる。

#### 【0053】

また、本実施の形態では、機器 4 を金庫、カードアプリとして鍵アプリを想定したが、機器 4 をビデオやセットトップボックス（STB）、カードアプリとして、決済カードアプリや、有料放送録画予約アプリ、有料放送受信操作アプリを想定してもよい。こうすることにより、正しく玄関の鍵の処理をしていないと、STB（PC）を介した決済処理（決済カードアプリ）ができない、ビデオ録画予約（その解除）（有料放送録画アプリ）ができない、といったサービスも可能である。

また、機器 4 を車の防犯モジュールとした場合、正しく玄関の鍵を閉じる処理をしたカードアプリと防犯モジュール（機器 4）で正しいチェックイン処理をしないまま、車のドアを開けたり、車のエンジンをかけたり、車のオーディオを外したりすると防犯ベルが鳴るといったサービスも可能である。

#### 【0054】

なお、実施形態では、主に、IC カードを携帯電話に装着する場合について説明したが、本発明はこれに限定されるものではない。携帯電話に代えて、PDA（Personal Digital Assistant）、メール端末、小型パーソナルコンピュータ、ゲーム機など、各種の端末装置・情報処理装置を用いることができる。また、IC カードは、国際標準規格を満たすものでも、満たさないものでも使用可能である。セキュアデバイスの形状は、カード状でもチップ状でも良く、情報処理装置に埋め込む形態であっても良い。

また、IC カードは接触通信手段のみを有しても良い。

#### 【産業上の利用可能性】

#### 【0055】

本発明は、各種のセキュアデバイスの機能や、各種の端末、装置、機器等の機能を場所、経路、位置等との関連で変える場合に利用することができ、オフィス、家庭、医療現場、教育現場など、あらゆる分野での利用が可能である。

#### 【図面の簡単な説明】

#### 【0056】

【図 1】 本発明の第 1 の実施形態における携帯電話、コンビカード及びゲートの構成を示すブロック図

【図 2】 本発明の第 1 の実施形態における認証情報 DB のデータ構成を示す図

【図 3】 本発明の第 1 の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス

【図 4】 本発明の第 1 の実施形態における携帯電話、IC カード及びゲートの構成を示すブロック図

【図5】本発明の第2の実施形態における携帯電話、コンビカード及びゲートの構成を示すブロック図

【図6】本発明の第2の実施形態における認証情報DBのデータ構成を示す図

【図7】本発明の第2の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス

【図8】本発明の第2の実施形態における優先度設定DBのデータ構成を示す図

【図9】本発明の第2の実施形態における優先度設定DBの他のデータ構成を示す図

【図10】本発明の第3の実施形態におけるドア、ICカード及びゲートの構成を示すブロック図

【図11】本発明の第3の実施形態におけるドア、ICカード及びゲートの動作を示すシーケンス

【図12】本発明の第3の実施形態におけるPIN入力部を持つドア、ICカード及びゲートの構成を示すブロック図

【図13】本発明の第3の実施形態におけるPIN入力部を持つドア、ICカード及びゲートの動作を示すシーケンス

【図14】本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の構成を示すブロック図

【図15】本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス

【図16】本発明の第4の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス

【図17】本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス（図16の続き）

【図18】本発明の第4の実施形態における携帯電話、コンビカード及びゲートの動作を示すシーケンス

【図19】本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス（図18の続き）

【図20】本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス

【図21】本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス

【図22】本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス

【図23】本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス

【図24】本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス

【図25】本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス

【図26】本発明の第4の実施形態における携帯電話、コンビカード、ゲート及び金庫の動作を示すシーケンス

【符号の説明】

【0057】

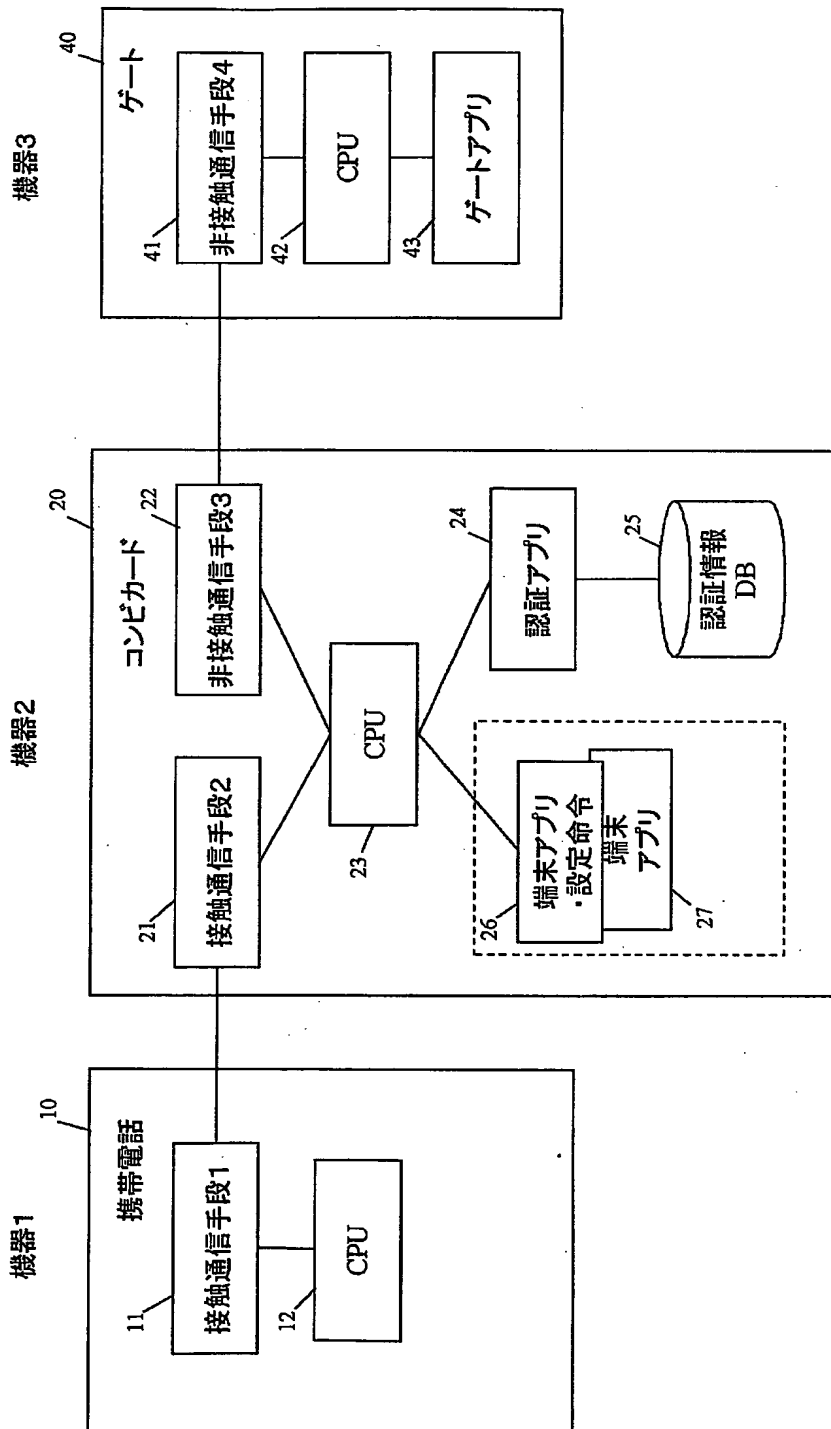
- 10 携帯電話
- 11 接触通信手段（
- 12 CPU
- 13 ローカル通信手段
- 14 端末アプリ
- 15 PIN入力部
- 20 コンビカード



21 接触通信手段  
22 非接触通信手段  
23 CPU  
24 認証アプリ  
25 認証情報DB  
26 端末アプリ・設定命令セット  
27 端末アプリ  
28 カードアプリ  
29 PINDB  
40 ゲート  
41 非接触通信手段  
42 CPU  
43 ゲートアプリ  
44 通信手段  
50 金庫  
51 非接触通信手段  
52 CPU  
53 鍵アプリ  
100 ドア  
200 ICカード

【書類名】 図面

【図1】

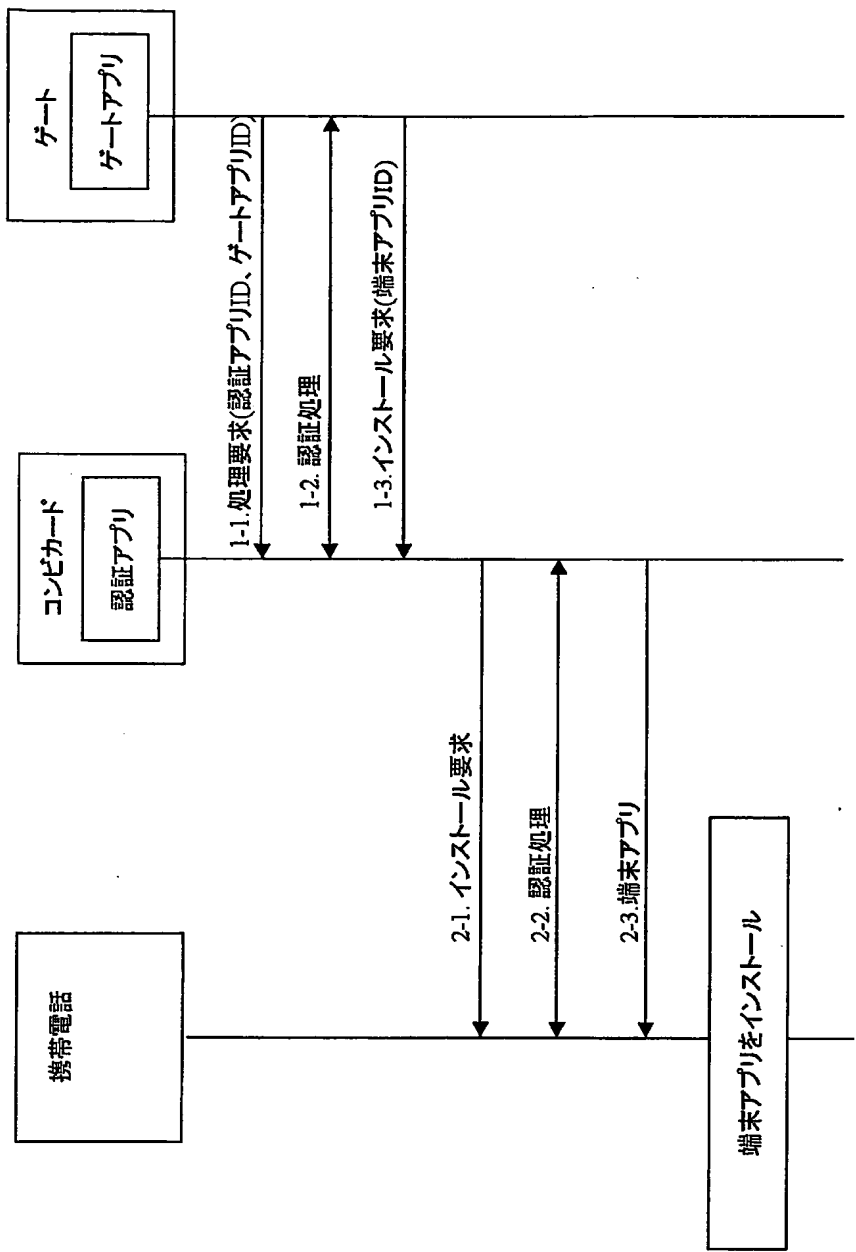


【図 2】

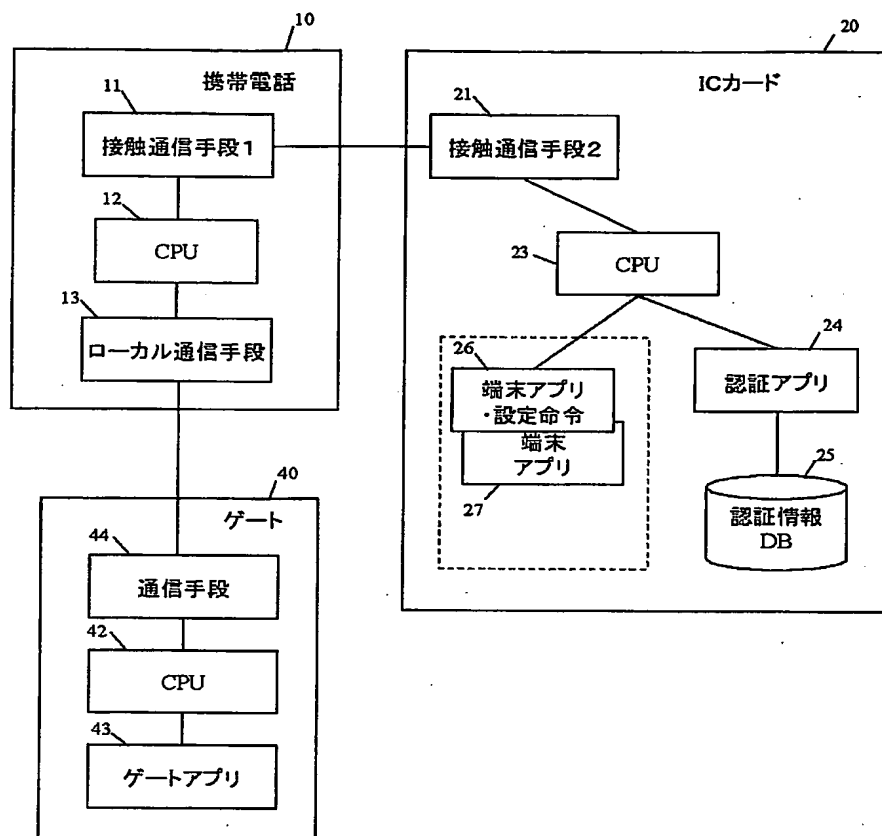
認証情報DB

ゲートアプリID	認証情報	インストール可能な端末アプリID、設定命令ID
www.app.co.jp/gate1		端末アプリ1ID 端末アプリ2ID 設定命令5ID

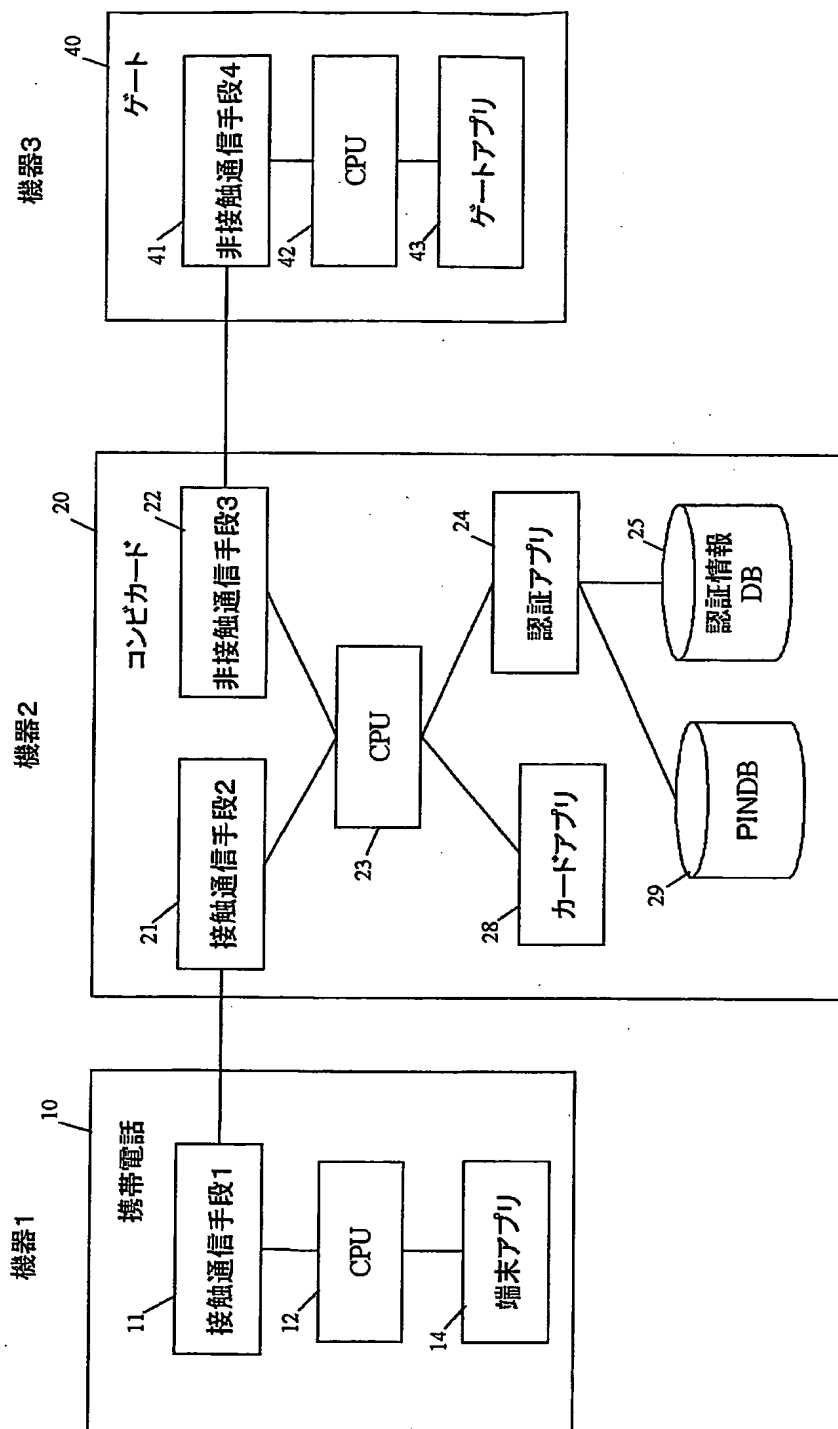
【図3】



【図 4】



【図 5】

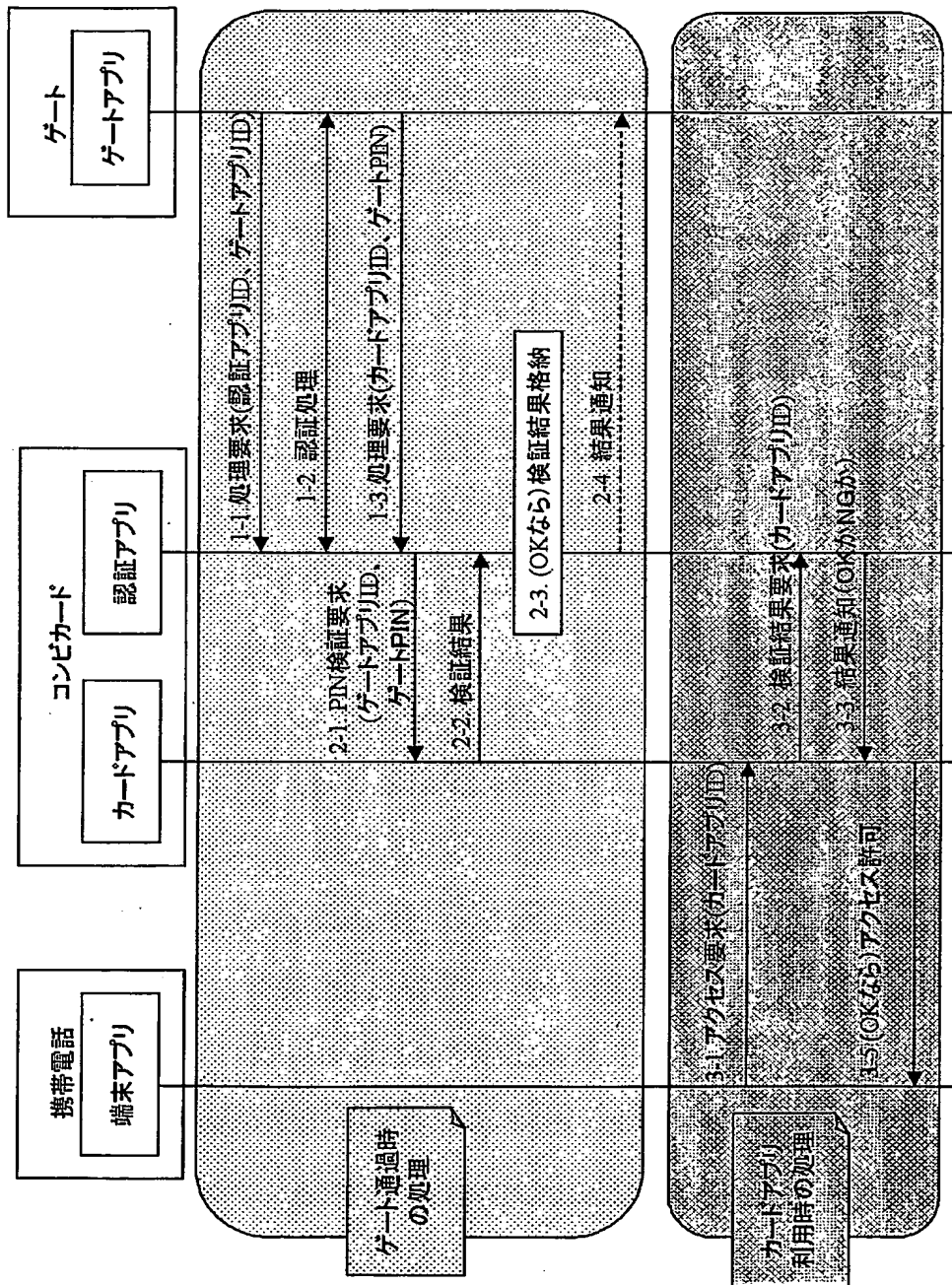


【図6】

認証情報DB

アプリID	認証情報	PIN設定可能なカードアプリID	PIN設定を解除するカードアプリID
www.app.co.jp/gate1		カードアプリ1ID カードアプリ2ID	カードアプリ3ID カードアプリ4ID

【図7】





【図8】

アプリID	優先度設定可能なカードアプリID	優先度設定を解除できるカードアプリID
www.app.co.jp/gate1	カードアプリ1ID カードアプリ2ID	カードアプリ3ID カードアプリ4ID

【図9】

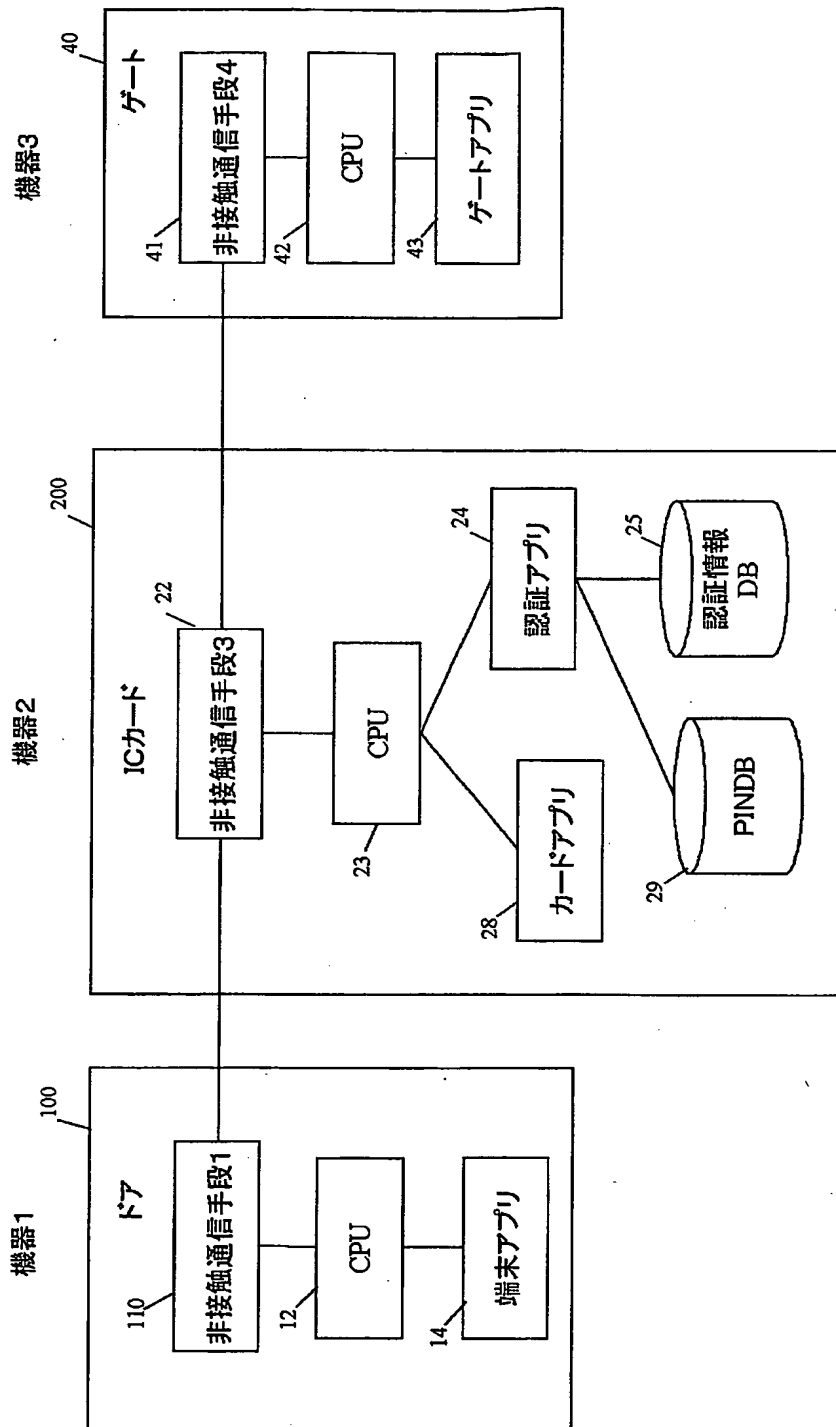
アプリID	設定可能な優先度テンプレート	解除可能な優先度テンプレート
www.app.co.jp/gate1	テンプレート1のID テンプレート2のID	テンプレート3のID

(a)

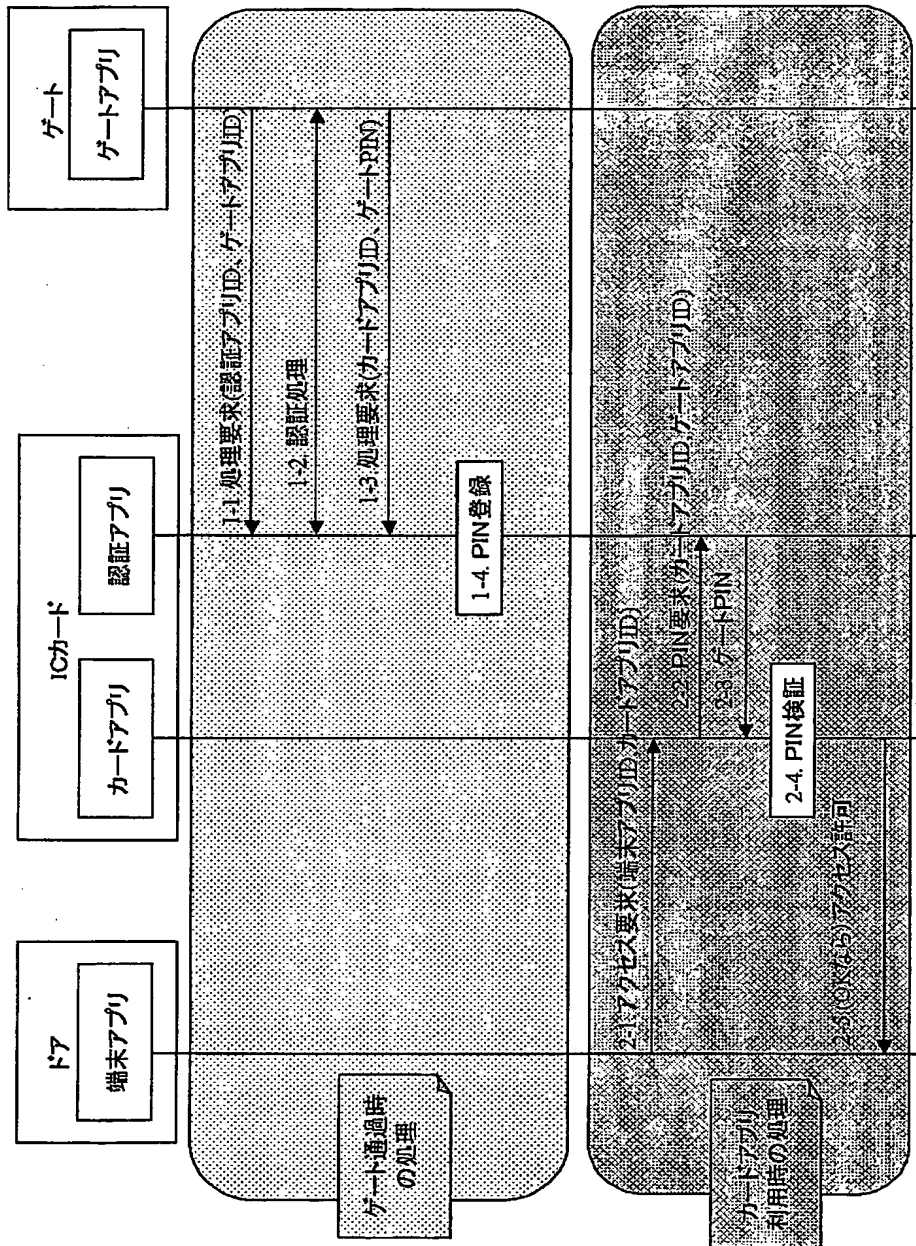
優先度テンプレートID	5
優先度1	カードアプリ1のID
優先度2	カードアプリ3のID

(b)

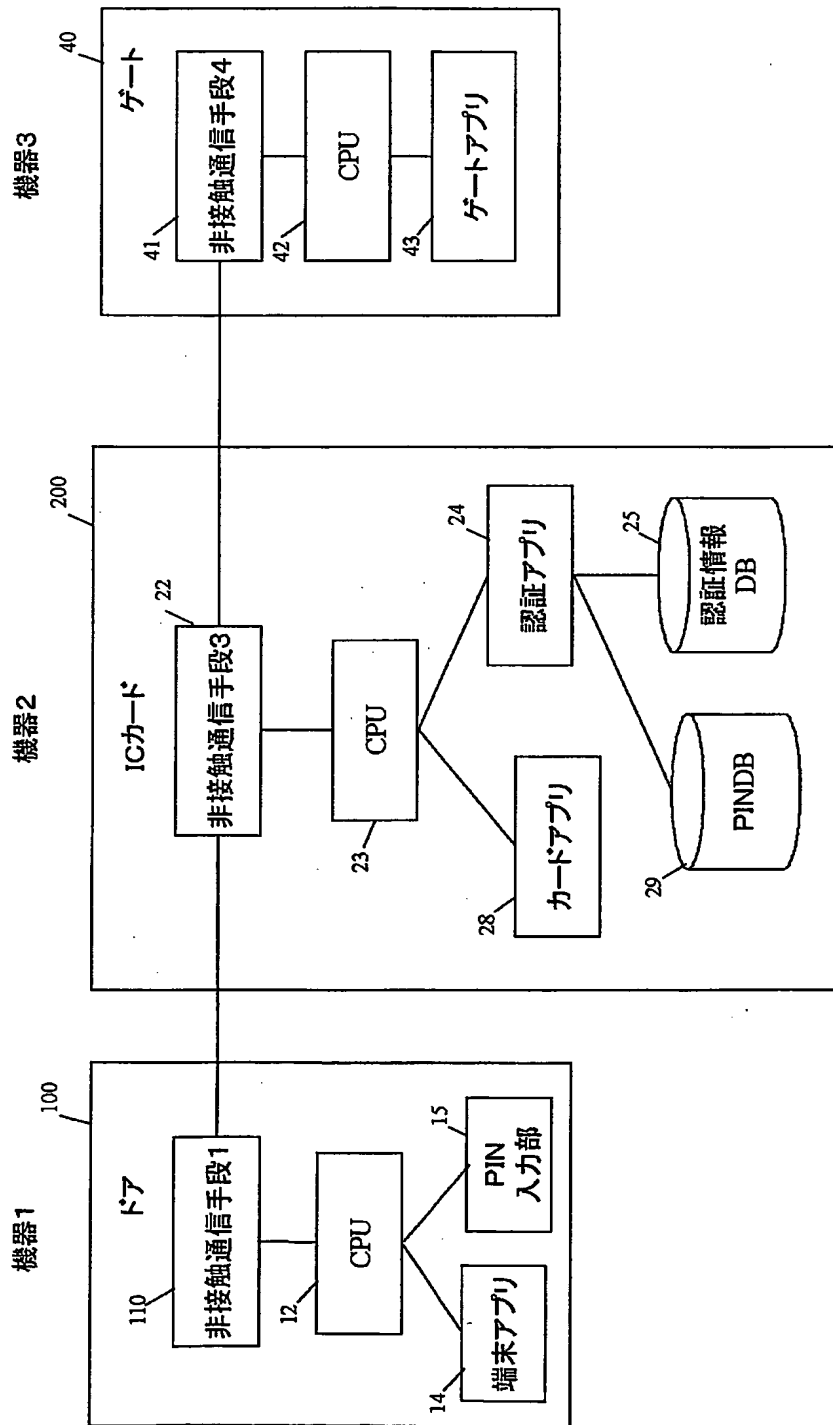
【図10】



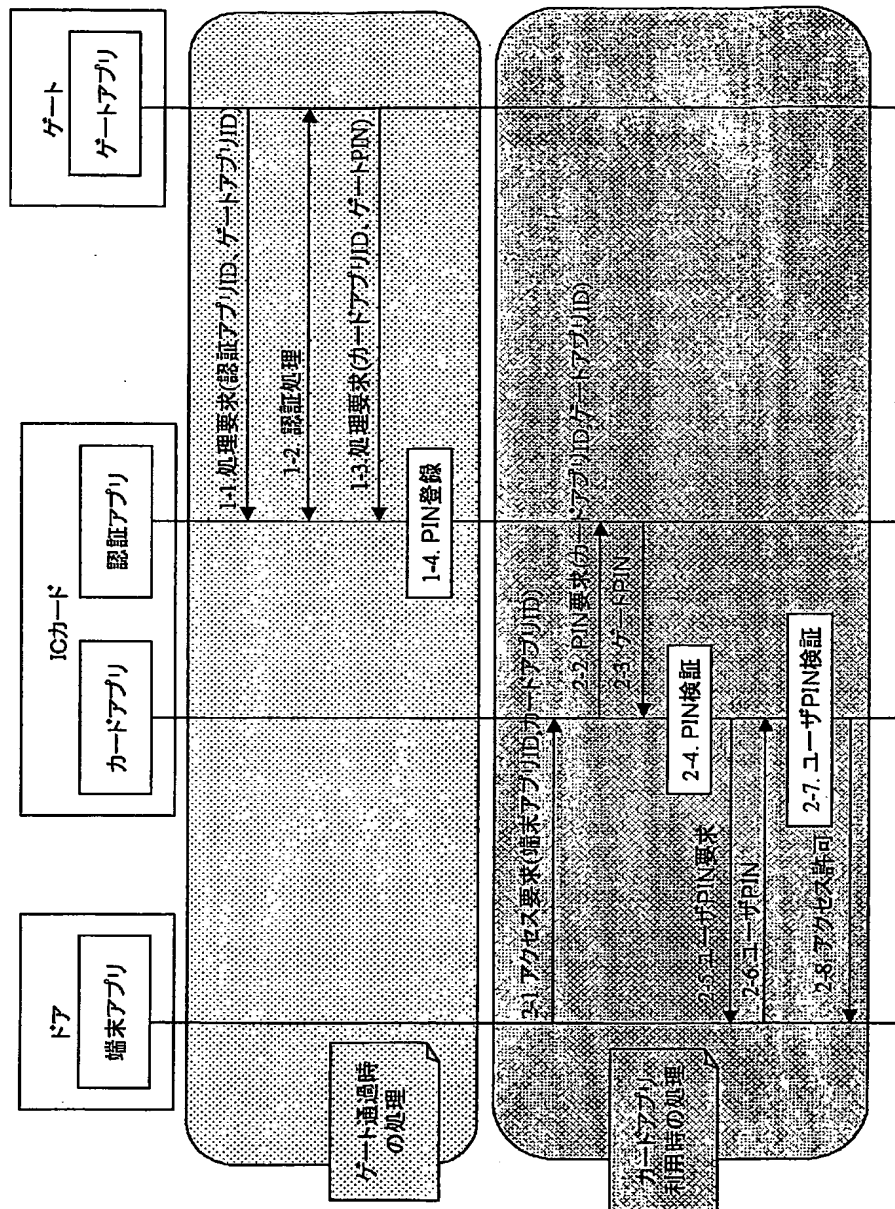
【図 11】



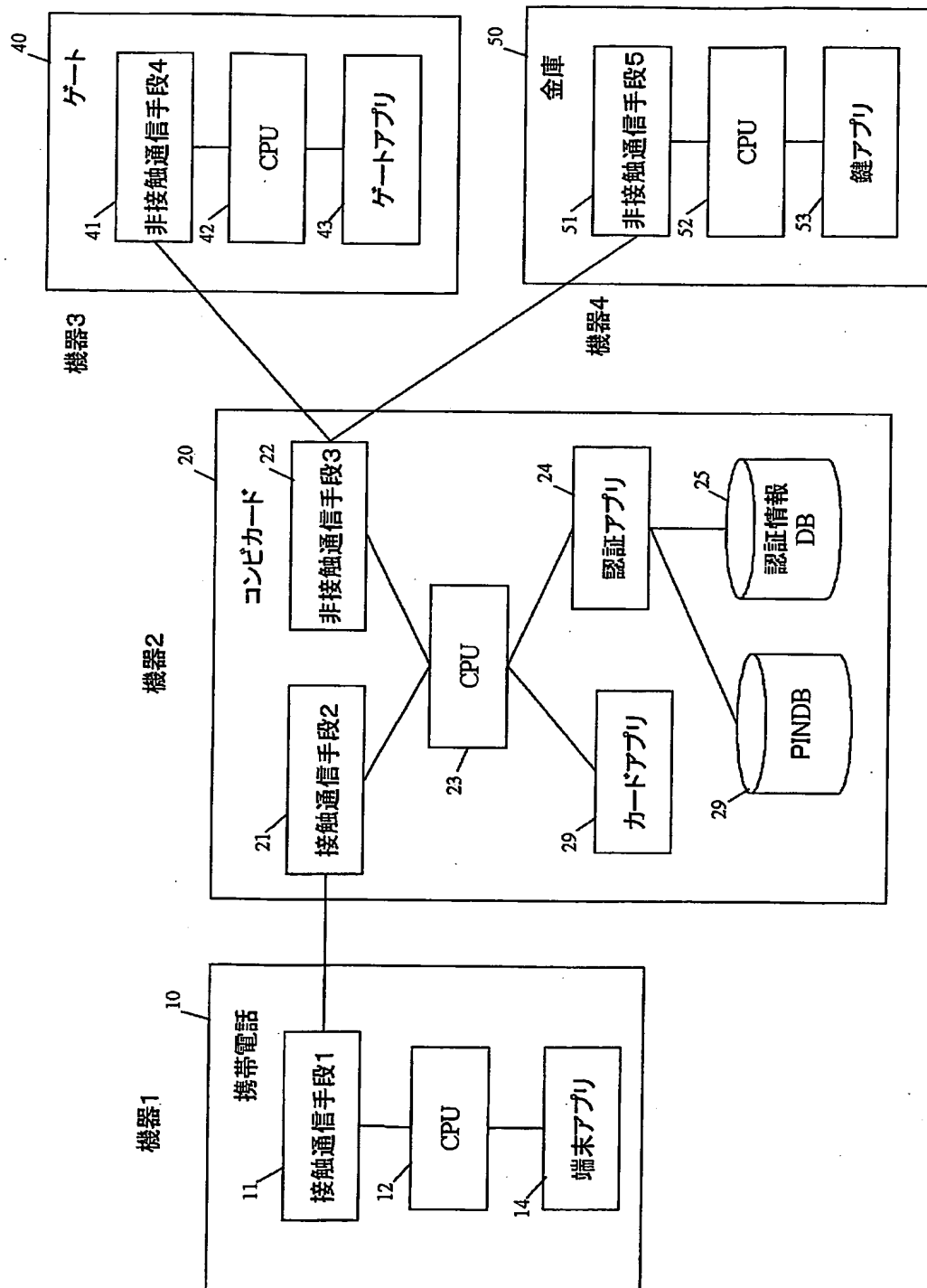
【図12】



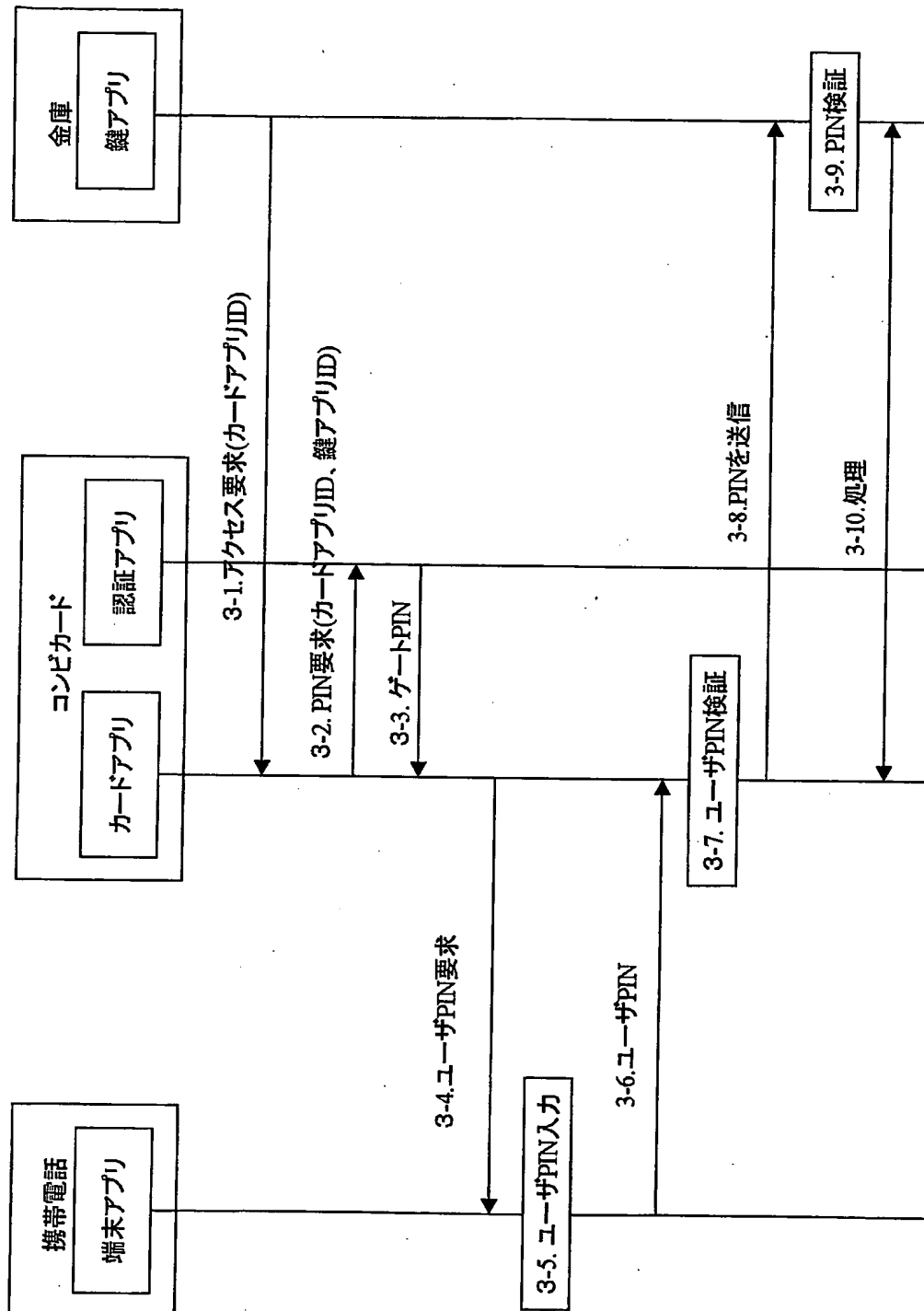
【図 13】



【図14】

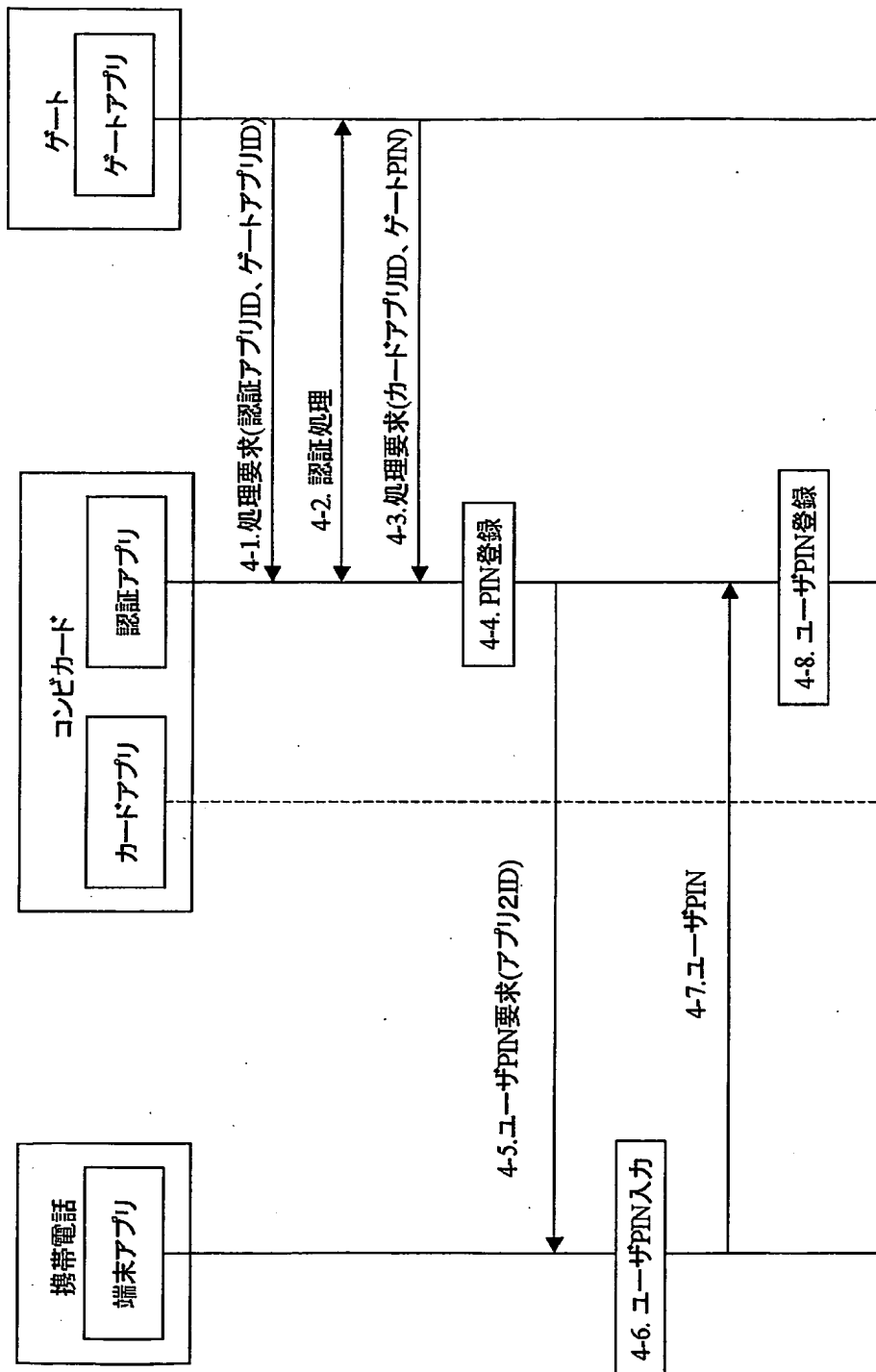


【図15】

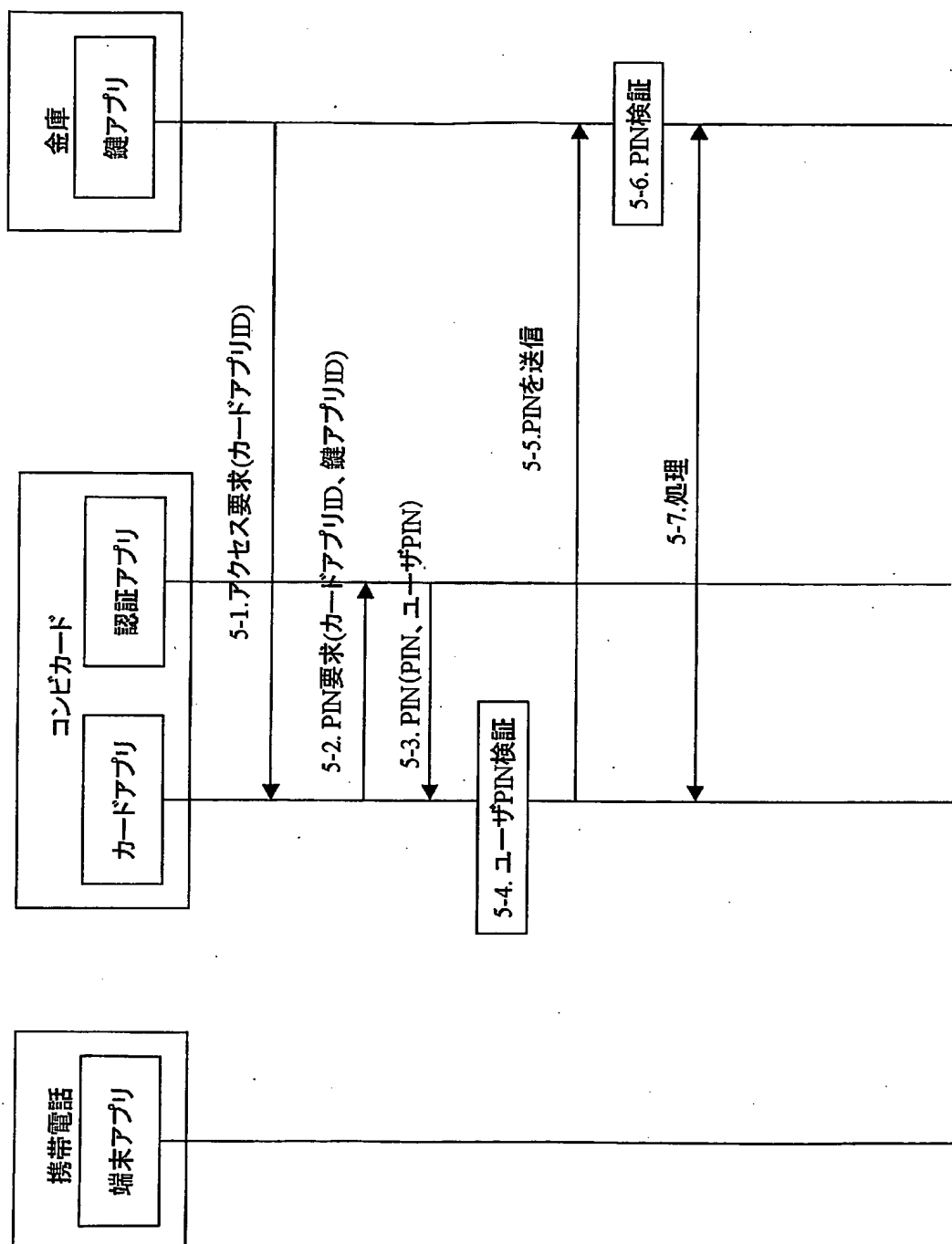




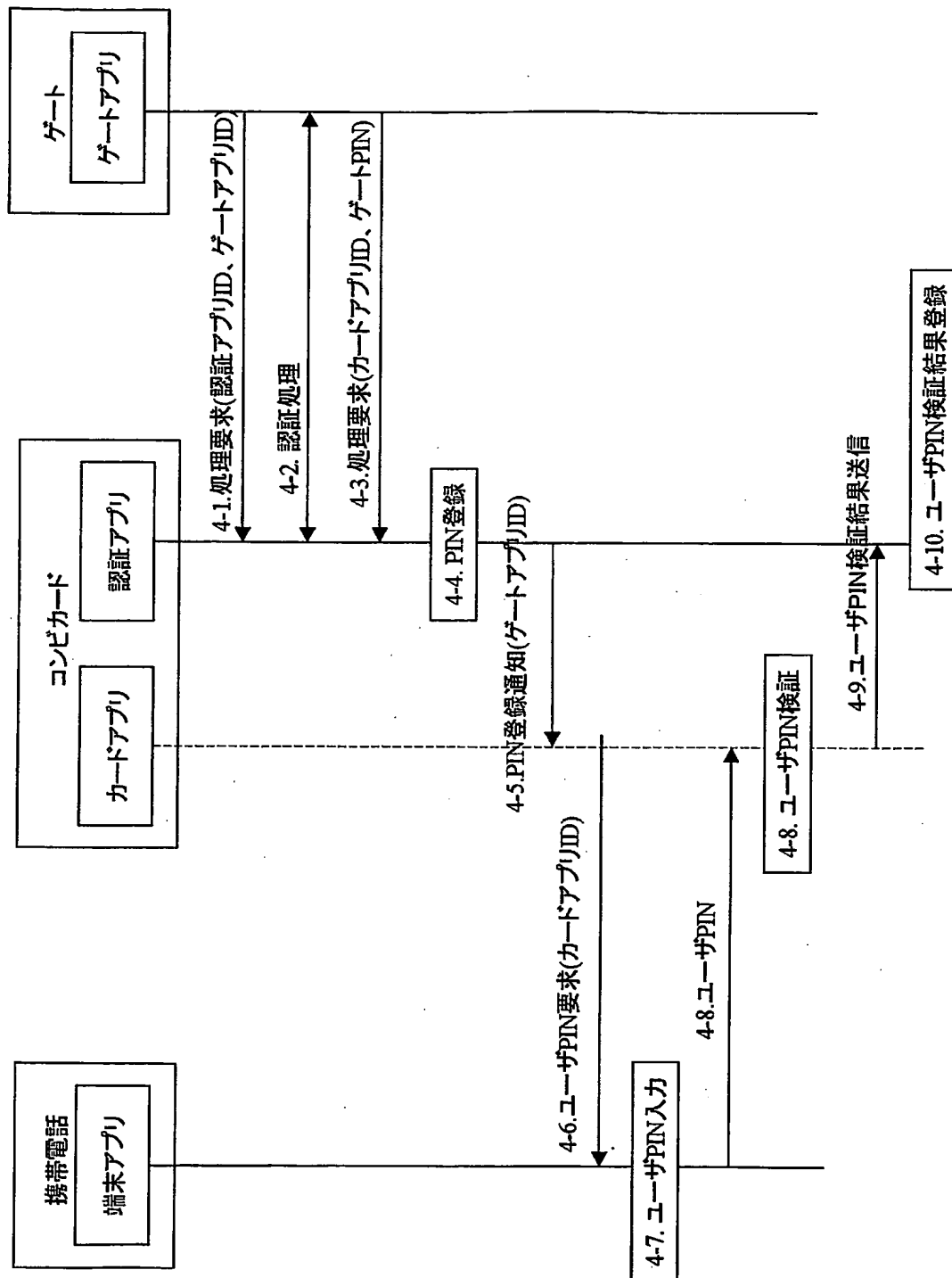
【図 16】



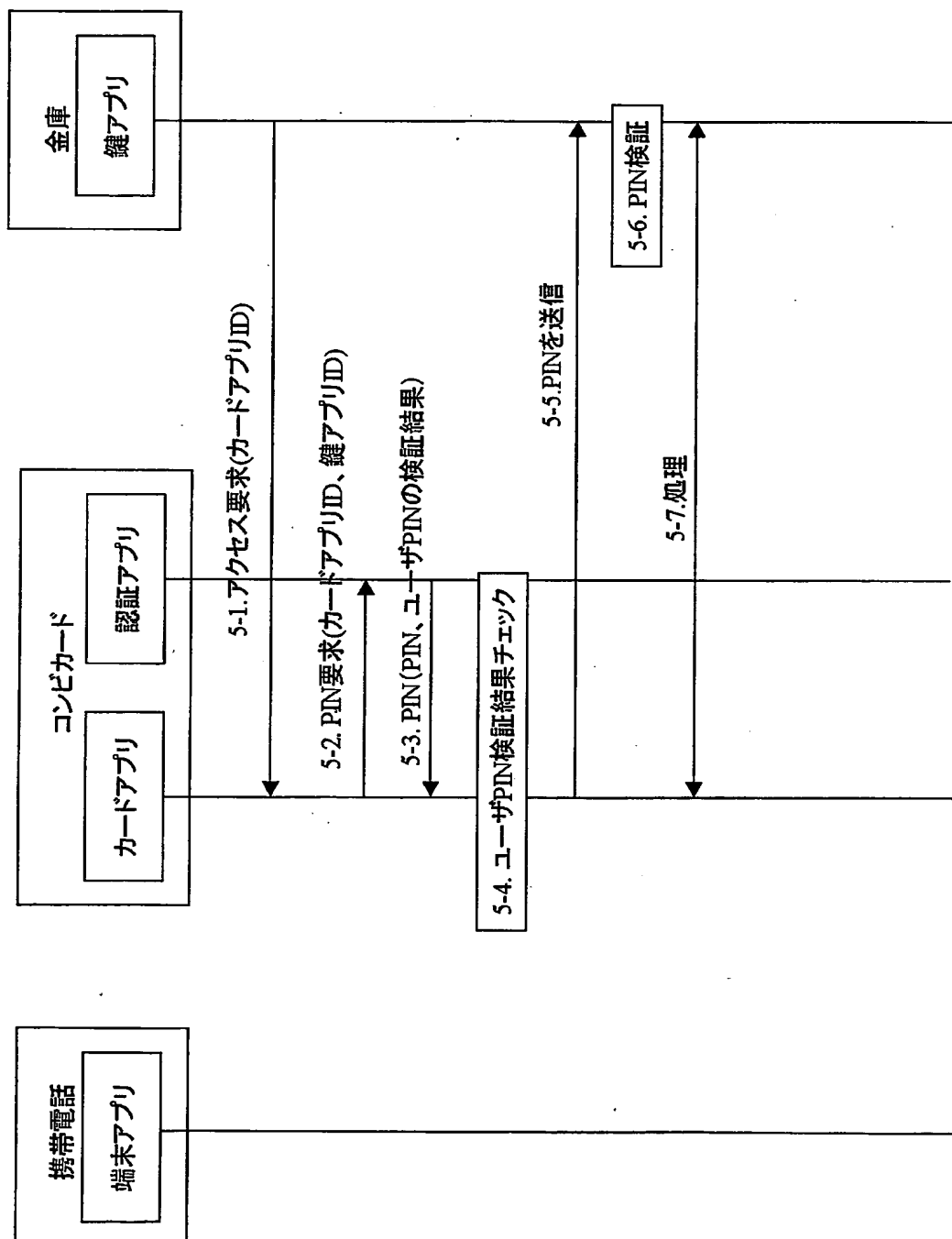
【図 17】



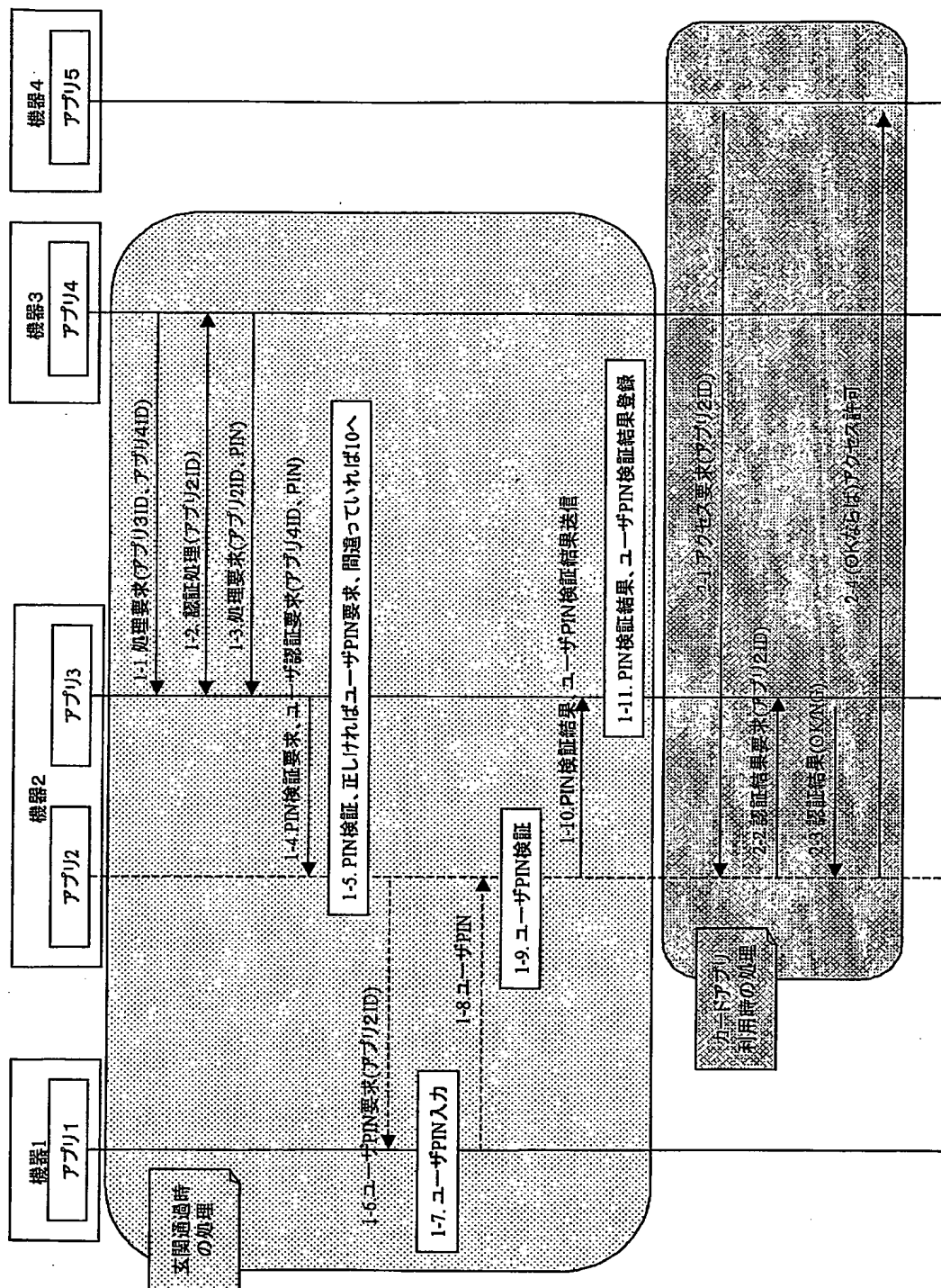
【図 18】



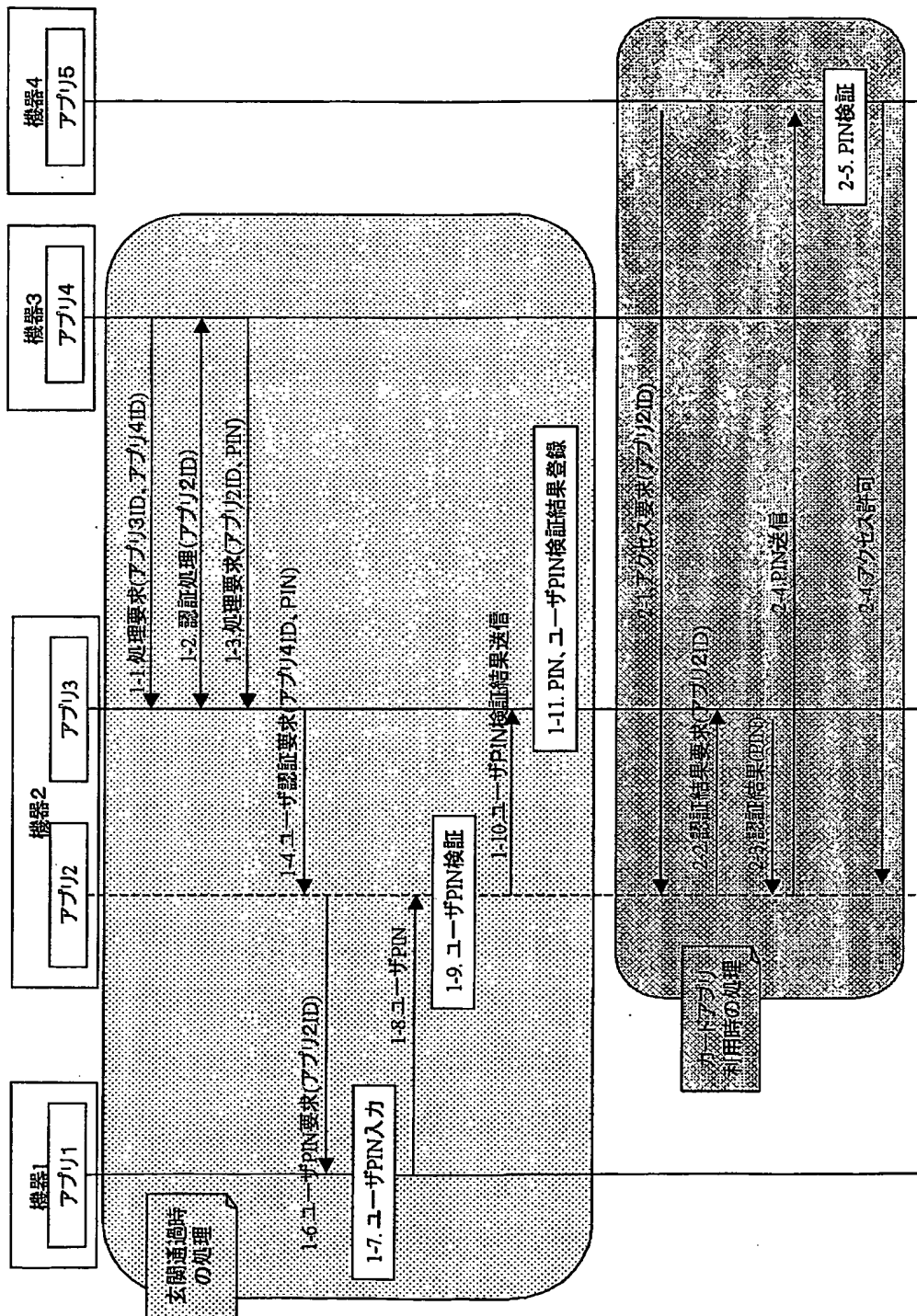
【図19】



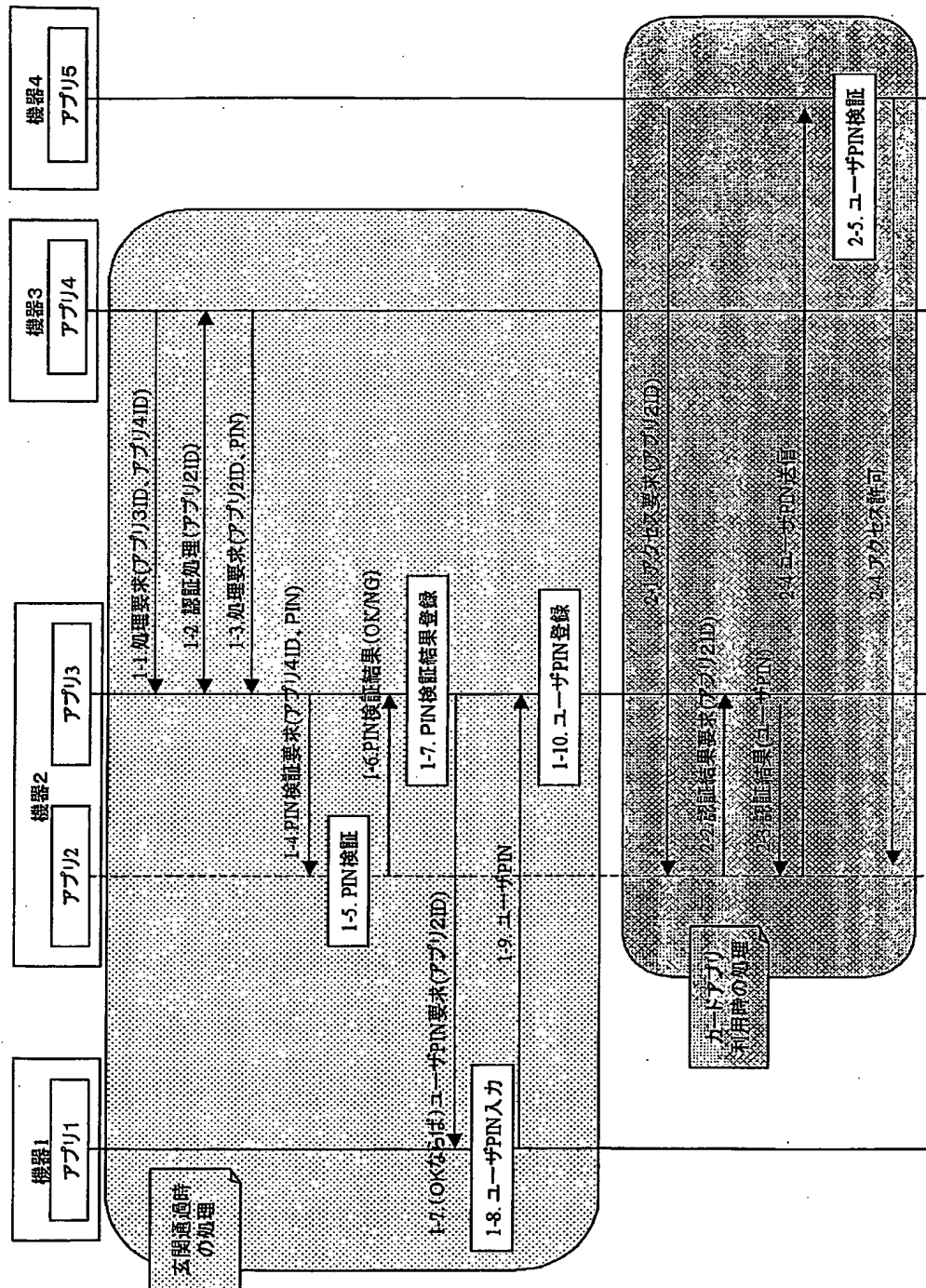
【図 20】



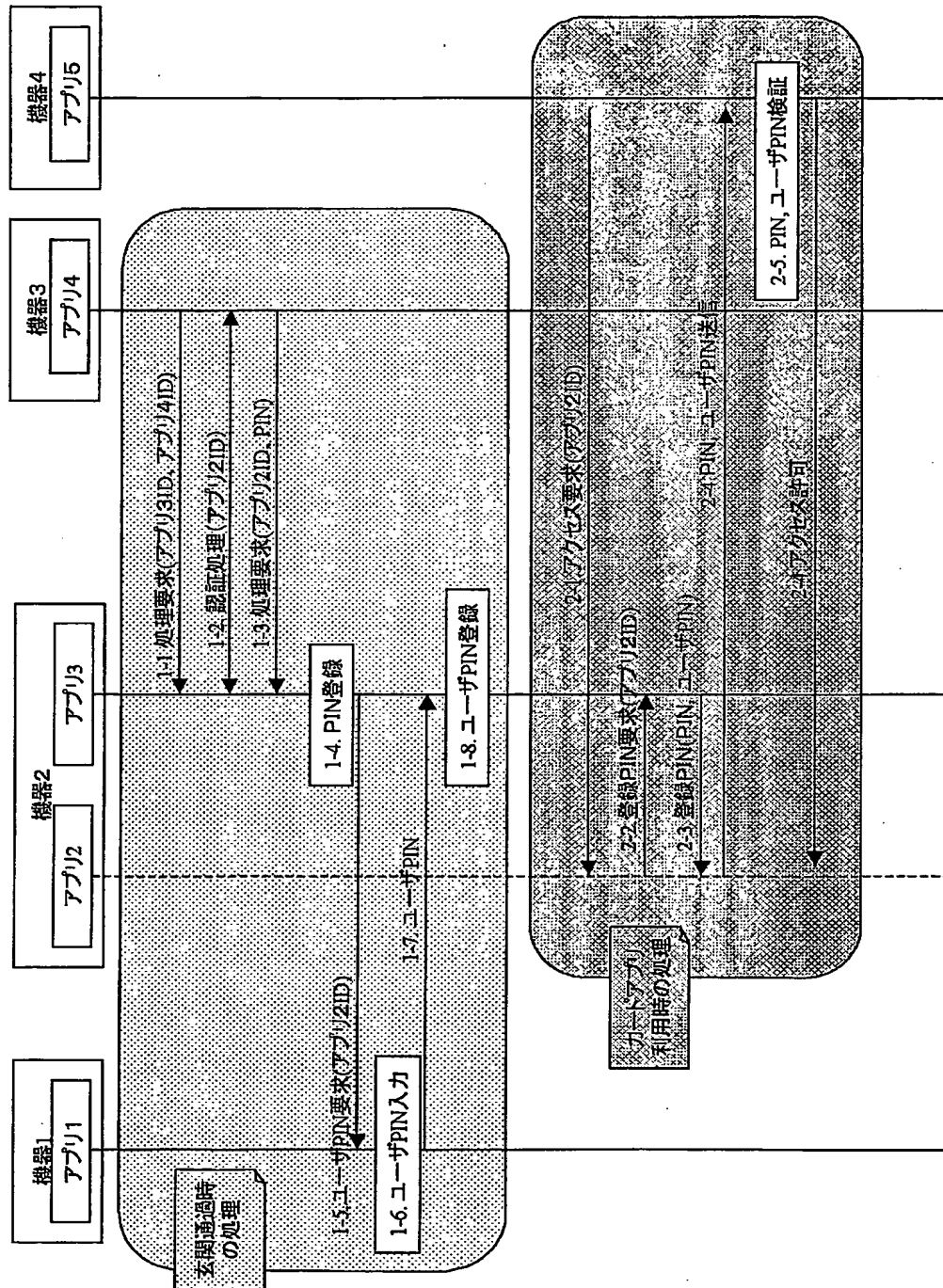
【図21】



【図22】

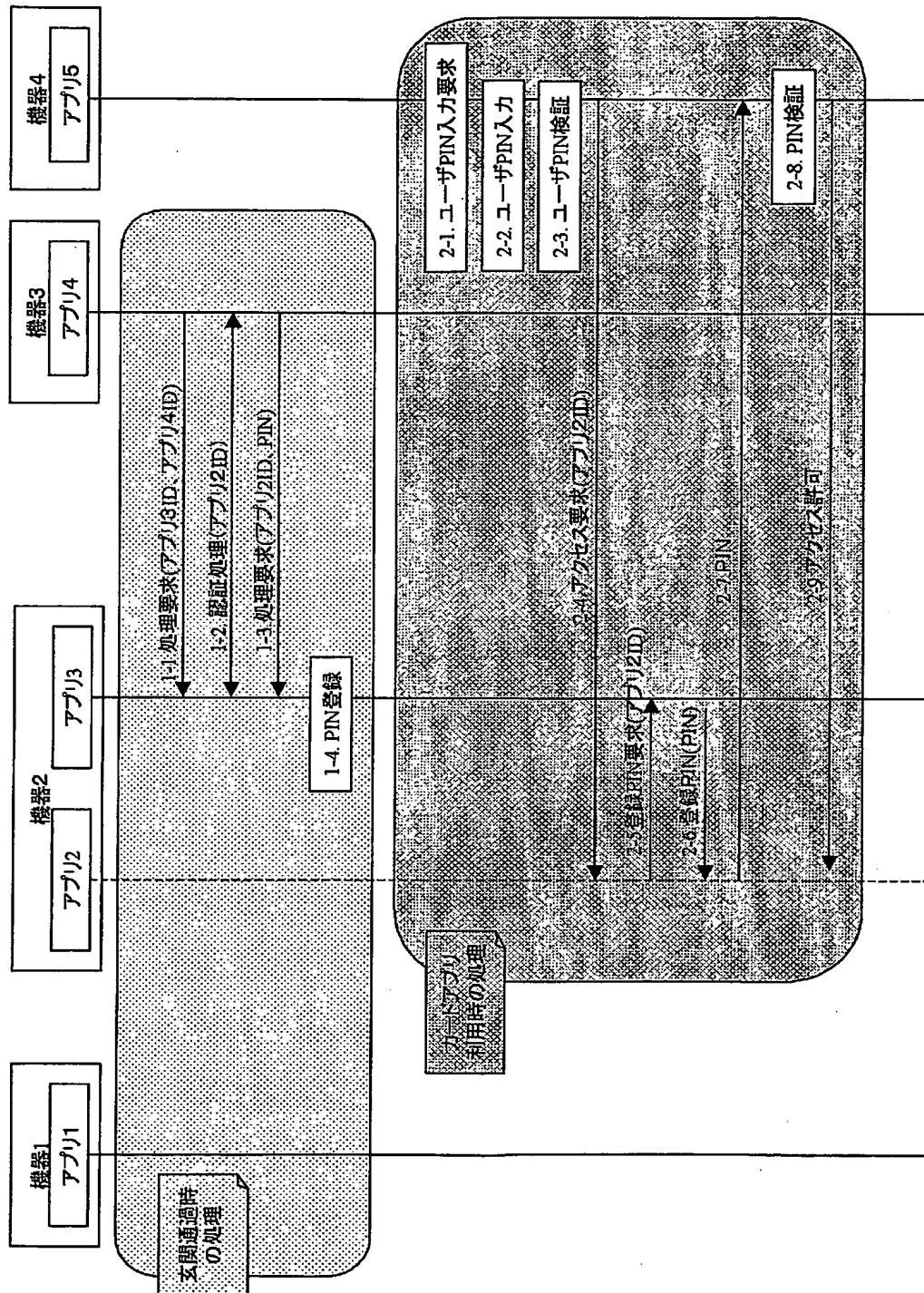


【図23】

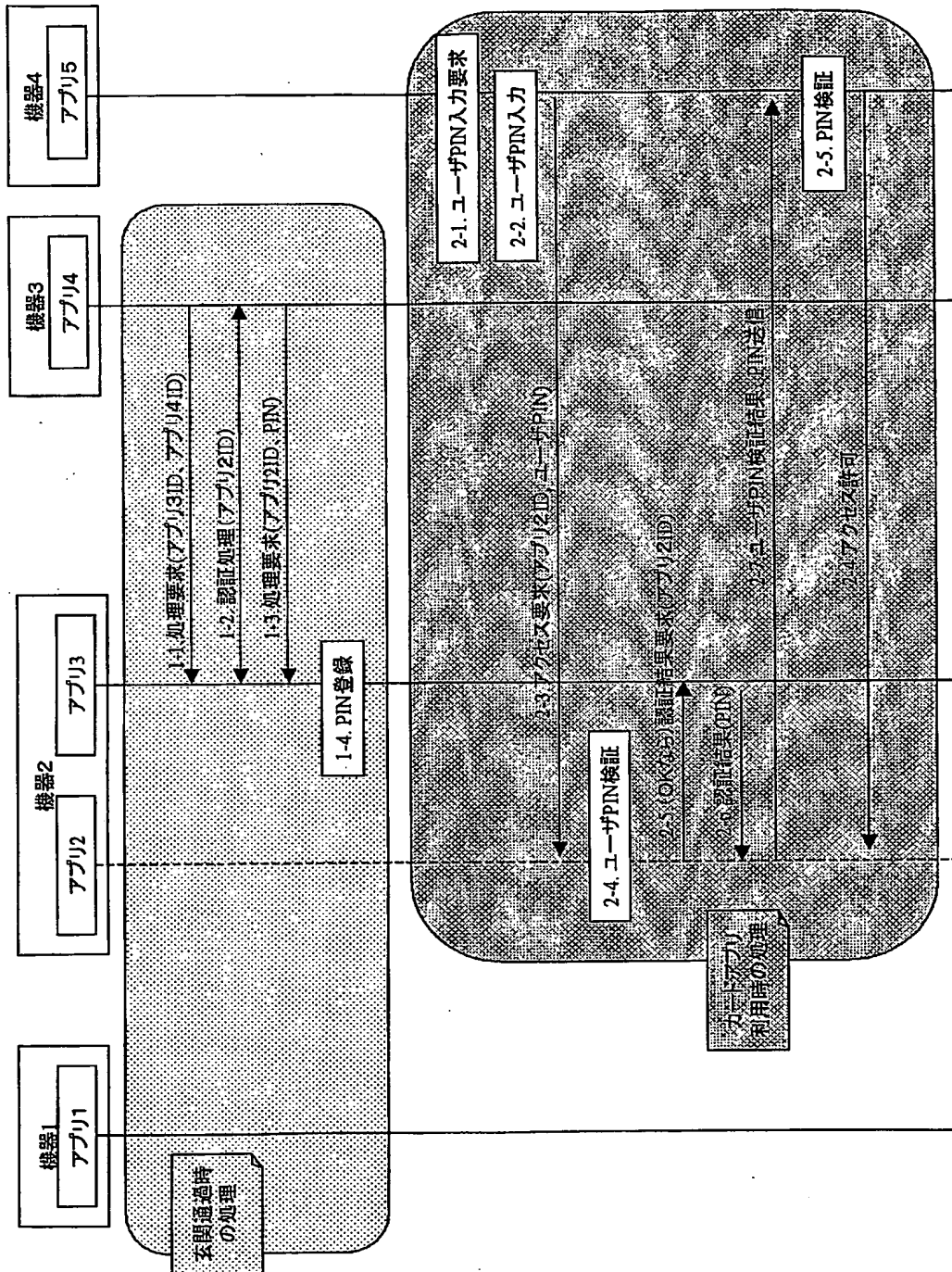




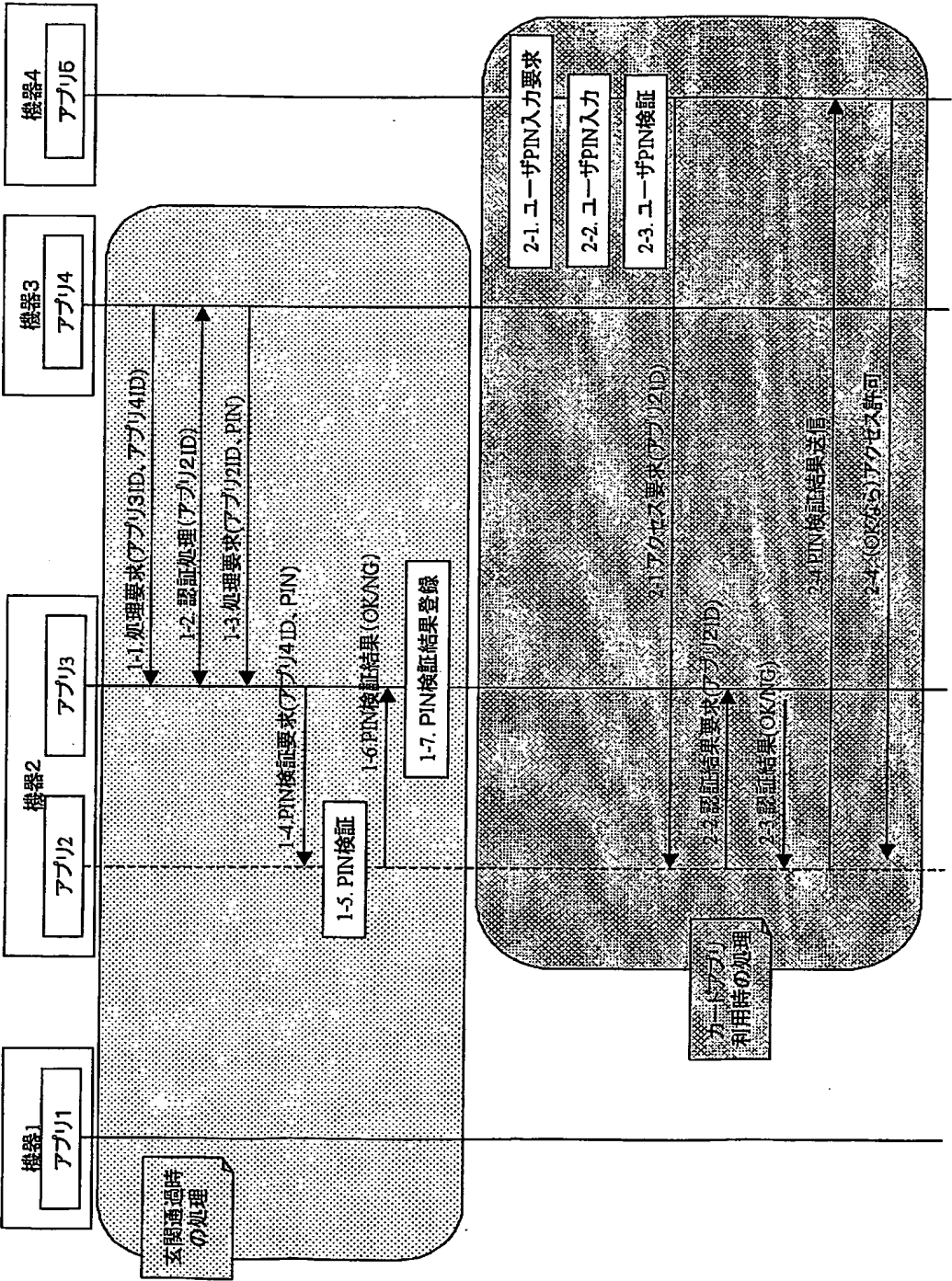
【図24】



【図25】



【図26】



**【書類名】 要約書****【要約】**

**【課題】** カードアプリ機能や装置機能等が発現されるエリアを限定できる IC カード等のセキュアデバイスを提供する。

**【解決手段】** セキュアデバイス 20 に、ゲート機器 40 に対して認証処理を行う認証手段 24 と、端末 10 にインストールする端末アプリ 26、27 と、認証手段 24 がゲート機器 40 との認証に成功した場合に、ゲート機器 40 から指定された端末アプリを端末 10 にインストールする制御手段 23 とを設けている。セキュアデバイス 20 をゲート機器 40 に翳し、正常に通過したエリアでのみ、端末アプリ 26、27 が端末 10 にインストールされる。ゲート機器 40 のゲートアプリ 43 が特定の領域で機能するアプリを指定するので、ユーザの登録操作等は不要であり、また、端末への GPS 受信機等の装備も必要がない。

**【選択図】 図 1**

特願 2004-019461

出願人履歴情報

識別番号

[000005821]

1. 変更年月日

1990年 8月28日

[変更理由]

新規登録

住 所

大阪府門真市大字門真1006番地

氏 名

松下電器産業株式会社